Externer Zugriff auf Nuclos

Sprache: **Deutsch** · English

Externer Zugriff auf Nuclos

> **Nuclos extern bereitstellen – HTTPS/NAT, Reverse Proxy oder VPN im Vergleich mit Vor- und Nachteilen.**

KONZEPT | ADMINISTRATOR | STAND: JUL 2026 | GILT FUER NUCLOS 4.2026.X

Auf dieser Seite

Es gibt drei Methoden, eine Nuclos-Instanz extern verfügbar zu machen.

1. Zugriff per HTTPS (NAT)

Port 443 wird per NAT an den Nuclos-Server weitergereicht; in Nuclos muss HTTPS konfiguriert sein. Ein abweichender Port ist möglich (dann stets angeben, z.B. `https://nuclos.firma.tld:8443`).

Vorteile	Nachteile
Einfache Konfiguration, keine extra Hardware.	Tomcat-Startseite von außen erreichbar; HTTPS-Port mit einer Anwendung belegt.

2. Zugriff über einen Reverse Proxy

Port 443 wird auf den Reverse Proxy geleitet, der die Anfragen filtert und weiterreicht. So lassen sich über verschiedene (Sub-)Domains mehrere Instanzen ansprechen – ideal, wenn Port 443 bereits belegt ist (siehe Reverse-Proxy-Konfiguration).

Vorteile	Nachteile
Mehrere Anwendungen unter einem Port; Unterscheidung per Subdomain; kein VPN-Client nötig.	Extra VM/Hardware; anspruchsvollere Konfiguration.

3. Zugriff über VPN (empfohlen)

Benutzer bauen eine VPN-Verbindung auf und greifen wie intern verschlüsselt zu. Bei korrekter Konfiguration das höchste Sicherheitsniveau; ohne VPN-Router genügt ein OpenVPN-Server auf dem Nuclos-Server.

Vorteile	Nachteile
Höchstes Sicherheitsniveau; keine Umstellung für Mitarbeiter; ggf. kompletter Netzzugriff.	VPN-Client muss installiert sein.

> **Kein HTTP nach außen**
>
> Zugriff per **HTTP** (unverschlüsselt) sollte für externe Verbindungen nie verwendet werden.

Verwandte Seiten

Betrieb von Nuclos hinter einem ReverseProxy

Proxy.

SSL-Verschlüsselung

SSL.

Öffnen

Öffnen