NETORYX
NETWORK MONITORING

Dokumentation

Lokal gehostetes Network-Monitoring

Angabe	Wert
Produkt	NETORYX – Network Monitoring
Version	1.0.1 (Vollversion)
Editionen	Ubuntu · Debian · Docker · Windows
Stand	November 2026 (Version 1.0.1 vom 18.11.2026)
Herausgeber	NETORYX – Luca Lindner & Thiemo Hechenblaikner
Kontakt	info@netoryx.at

Wichtiger Hinweis zur Funktionsgarantie

Wir können nicht garantieren, dass NETORYX in jeder Umgebung zu 100 % fehlerfrei funktioniert.

Sollten Fehler auftreten, melden Sie diese bitte **so früh wie möglich** – entweder auf der Website im Bereich **Community** oder per E-Mail an **info@netoryx.at**. Wir sehen uns jedes Problem so schnell wie möglich an.

Inhaltsverzeichnis

1. Was ist NETORYX? ... 3
1.1 Die wichtigsten Eigenschaften ... 3
1.2 Wichtige Begriffe ... 3
2. Die vier Editionen ... 4
3. Funktionsumfang ... 4
4. Architektur ... 5
5. Systemanforderungen ... 6
5.1 Linux (Ubuntu, Debian, Docker) ... 6
5.2 Windows Server ... 6
6. Installation ... 7
6.1 Ubuntu Server 22.04 / 24.04 ... 7
6.2 Debian 12 / 13 ... 7
6.3 Docker ... 7
6.4 Windows Server ... 7
6.5 Erste Anmeldung und Einrichtung ... 8
6.6 Firewall ... 8
7. Bedienung ... 8
7.1 Oberfläche ... 8
7.2 Prüfungen ... 9
7.3 Systemressourcen und Windows-Updates ... 9
7.4 Benutzer und Anmeldung ... 9
7.5 Benachrichtigungen ... 9
7.6 Befehlszeile (CLI) ... 10
8. Betrieb und Wartung ... 10
8.1 Zertifikate ... 10
8.2 Sicherung und Wiederherstellung ... 10
8.3 Update, Neustart, Werkseinstellungen ... 10
8.4 Große Installationen ... 10
9. Eigene Prüfungstypen (Plugins) ... 10
10. Datenschutz, Lizenz und Drittkomponenten ... 11
10.1 Datenschutz ... 11
10.2 NETORYX-Lizenz 1.0 ... 11
10.3 Drittkomponenten ... 11
11. Testumgebung und Testergebnisse ... 11
11.1 Testumgebung ... 12
11.2 Protokolle und Prüfungen ... 12
11.3 Oberfläche, Benachrichtigungen und Benutzer ... 12
11.4 Einstellungen und System ... 13
11.5 Offene Punkte ... 13
12. Fehler melden und Support ... 14
12.1 So melden Sie einen Fehler ... 14
Anhang: Mitgelieferte Dokumente ... 14

1. Was ist NETORYX?

NETORYX ist ein lokal gehostetes Network-Monitoring. Es läuft auf einem eigenen Server im eigenen Netz, braucht **keine Cloud**, sendet **keine Telemetrie** und prüft Geräte in festen Intervallen (ab 15 Sekunden). Backend, Frontend und Einrichtung sind in einem Paket zusammengefasst.

Die Oberfläche ist eine Web-Anwendung (React) in **Deutsch und Englisch** mit hellem und dunklem Design. Gespeichert wird in einer lokalen SQLite-Datenbank; Zugangsdaten und Sicherungen sind AES-verschlüsselt.

1.1 Die wichtigsten Eigenschaften

- **Echte Netzwerk-Checks:** PING, TCP, HTTP/HTTPS, NTP, SMTP und SNMP (v1/v2c/v3).
- **Systemressourcen:** CPU, RAM, Festplatte, Temperatur und PoE-Auslastung per SNMP; Windows-Rechner per WinRM ohne Agent.
- **Windows-Updates** per WinRM – ohne Administratorrechte mit einem normalen Dienstkonto.
- **Übersicht:** Dashboard, eigene Dashboards, Baumansicht, Ereignisse und Netzwerk-Log je Gerät.
- **Sichere Anmeldung:** lokal, Active Directory/LDAP oder Single Sign-On (OpenID Connect) mit Zwei-Faktor (Authenticator-App, Duo Push).
- **Benachrichtigungen** per E-Mail und Webhook mit Regeln je Ordner, Status und Risikostufe.
- **Verwaltung im Browser:** Zertifikate, Sicherung, Update, Neustart und Werkseinstellungen.
- **Skalierbar** bis 10.000 Geräte mit allen acht Prüfungsarten (je nach Edition).

1.2 Wichtige Begriffe

Begriff	Bedeutung
Gerät	Etwas, das überwacht oder dokumentiert wird (Switch, Access Point, Server, Client …).
Prüfung (Monitor)	Eine konkrete Überwachung an einem Gerät, z. B. „PING alle 60 s“. Ein Gerät kann beliebig viele Prüfungen haben.
Risikostufe	Wie kritisch ein Gerät ist (Critical, High, Medium, Low). Wird manuell vergeben.
Zustand	Wie es dem Gerät gerade geht (OK, Warnung, Ausfall, Pausiert) – ergibt sich aus den Prüfungen.
Ereignis	Ein bestätigter Statuswechsel einer Prüfung, z. B. von „Erreichbar“ zu „Ausfall“.
Kachel	Eine Prüfung in der Baumansicht, farbig nach Zustand (UP, WARNING, DOWN, PAUSED).
Vorlage	Voreinstellungen für einen Gerätetyp inklusive aller Prüfungen und Zugangsdaten.
Kanal / Regel	Wohin (E-Mail, Webhook) und wann benachrichtigt wird.

2. Die vier Editionen

NETORYX 1.0.1 gibt es in vier Editionen. Der Funktionsumfang ist praktisch gleich; unterschiedlich sind Betriebssystem, Installation und Update.

Edition	Zielsystem	Installation	Geräte (empfohlen)
Ubuntu	Ubuntu Server 22.04 LTS und 24.04 LTS	`sudo bash install.sh --domain <name>`	bis 10.000
Debian	Debian 12 (bookworm) und Debian 13 (trixie)	`bash install.sh --domain <name>` als root	bis 10.000
Docker	Linux-Host mit Docker Engine 24+ und Compose v2	`docker compose up -d --build`	bis 10.000 (Host-Netz ab ~2.500)
Windows	Windows Server 2016, 2019, 2022, 2025	`windows\install.ps1` in PowerShell als Administrator	bis 5.000

- **Pakete:** `Netoryx-Ubuntu-1.0.1.zip`, `Netoryx-Debian-1.0.1.zip`, `Netoryx-Docker-1.0.1.zip` und `Netoryx-Windows-1.0.1.zip`. Im ZIP liegt jeweils ein gleich benannter Ordner.
- **Web-Update:** Die Linux-Editionen nehmen nur Pakete der eigenen Edition an (Datei `EDITION`); Beta-Pakete und Pakete anderer Editionen werden abgelehnt.
- **Docker:** Update per neuem Image; Docker Desktop (Windows/macOS) nur zum Testen, bis etwa 250 Geräte.
- **Windows:** Ab etwa 2.500 Geräten sind zusätzliche Netzwerk-Einstellungen nötig, weil Windows nur 16.384 freie TCP-Absenderports bereithält. Für 5.000 bis 10.000 Geräte empfiehlt sich die Ubuntu- oder Docker-Edition.
- **Umstieg von der Beta:** Das Paket wird wie ein Update installiert – Daten, Domain und Zertifikat bleiben erhalten.

3. Funktionsumfang

Bereich	Umsetzung
Prüfungen	PING, HTTP/HTTPS, NTP, SNMP v1/v2c/v3, SMTP, TCP; Systemressourcen und Windows-Updates. Intervall ab 15 Sekunden.
Geräte	Name plus IP, Hostname, MAC, Standort, Hersteller, Beschreibung und Tags; pausierbar. Geräteseite mit Statistiken (CPU, RAM, Festplatte, Temperatur, Antwortzeiten, Verfügbarkeit bis 30 Tage).
Vorlagen	Gerätetypen einmal einrichten (inkl. Prüfungen und Zugangsdaten); sechs Beispielvorlagen per Klick.
Dashboard	Anklickbare Kennzahlen, Filter und Liste aller Ausfälle. Eigene Dashboards aus Bausteinen (Kennzahlen, Gerätelisten, Verlaufsgrafik mit bis zu 8 Linien, Notizen, Uhr …), privat oder für alle.
Baumansicht	Ordner → Geräte → je Prüfung eine farbige Kachel; Zählerleiste als Filter, Kachelgröße S bis XL, Verschieben per Drag & Drop.
Ereignisse & Netzwerk-Log	Statuswechsel filterbar nach UP/WARNING/DOWN/PAUSED; je Gerät jede einzelne Prüfung über mehrere Tage, mit CSV-Export.

Bereich	Umsetzung
Ordner	Beliebig tief; Klick öffnet ein Ordner-Dashboard inklusive aller Unterordner.
Import/Export	Ordner, Vorlagen und Geräte als JSON oder CSV (Excel), Import mit Vorschau, ohne Zugangsdaten.
Suche	Kopfzeile (Strg+K) findet Geräte, Ordner, Dashboards – Admins auch Vorlagen, Benutzer und Einstellungen.
Befehlszeile (CLI)	Alles, was die Oberfläche kann, auch per Befehl – im Browser (Symbol >_) und über SSH (`ssh netoryx-cli@<server>`). Hilfe mit `?`, Tab-Ergänzung, Verlauf, Skripte.
Benutzer	Administrator, Lesen & Schreiben, Nur Lesen – mit Ordner-Freigaben.
Anmeldung	Lokal, Active Directory/LDAP, Single Sign-On (z. B. Microsoft Entra ID, ADFS, Keycloak); Zwei-Faktor per Authenticator-App (TOTP) und/oder Duo Push.
Benachrichtigungen	E-Mail und Webhook, pro Gerät einschaltbar, Regeln je Ordner/Status/Risikostufe; E-Mails mit Signatur.
Verwaltung	Zertifikate (eigene CA, Let's Encrypt, Upload), Sicherung, Wiederherstellung, Update, Protokolle, Neustart, Werkseinstellungen.
Sicherheit	AES-verschlüsselte Zugangsdaten und Sicherungen, Downloads optional mit Passwort (AES-256-ZIP), Content-Security-Policy, Sperre nach Fehlversuchen.
Datenschutz	DSGVO/DSG: Datenschutzhinweise, Aufbewahrungsfristen, IP-Kürzung, Datenauskunft, Pseudonymisierung.

4. Architektur

NETORYX besteht aus einer statischen Web-Oberfläche, einem Webserver für HTTPS, einem Python-Backend mit Scheduler und einer lokalen Datenbank. Die Prüfungen werden vom Backend aktiv ausgeführt.



Prüfprotokolle: ICMP · HTTP/S · NTP · SNMP · SMTP · TCP · WinRM

Baustein	Wahl und Begründung
Backend	Python 3.10+ / FastAPI – gute Bibliotheken für echte Protokoll-Checks (icmplib, pysnmp, ntplib, pypsrp), asynchroner Scheduler.
Datenbank	SQLite (WAL) – kein eigener Dienst, konsistente Online-Backups; PostgreSQL über `NETORYX_DATABASE_URL` vorbereitet.
Frontend	React 18, Vite, TypeScript, TailwindCSS – statisch über nginx auslieferbar.
Diagramme	Eigene SVG-Komponenten, keine Chart-Bibliothek.
Anmeldung	JWT (HS256) und bcrypt, TOTP, ldap3, OpenID Connect.
Schriften	IBM Plex Sans/Mono, lokal eingebunden – keine externen Server.

Je Edition: Unter Ubuntu und Debian arbeiten nginx und systemd-Dienste; im Docker-Image laufen nginx, Backend, Prüf-Prozesse und ein Helfer unter `supervisord`. Unter Windows übernimmt der Dienst **NETORYX** (HTTPS direkt über uvicorn) zusammen mit dem Dienst **NETORYX-Helper** (Zertifikate, Neustart) – ohne IIS und nginx.

5. Systemanforderungen

Die Werte gelten für **alle acht Prüfungen je Gerät** (Ping, TCP, HTTP, NTP, SMTP, SNMP, Systemressourcen, Windows-Updates) mit Standard-Intervallen und Standard-Aufbewahrung. Der kleinste Server benötigt 2 CPU-Kerne, 2 GB RAM und 30 GB SSD.

5.1 Linux (Ubuntu, Debian, Docker)

Geräte	Messungen/Min.	Kerne	RAM	SSD	Prüf-Prozesse	Empfohlen
100	440	2	2 GB	30 GB	0	2 Kerne · 4 GB · 50 GB
500	2.200	2	2 GB	50 GB	0	2 Kerne · 4 GB · 80 GB
1.000	4.400	2	4 GB	60 GB	0	4 Kerne · 8 GB · 100 GB
2.500	11.000	4	4 GB	80 GB	2	4 Kerne · 8 GB · 150 GB
5.000	22.000	6	8 GB	120 GB	4	8 Kerne · 12 GB · 200 GB
7.500	33.000	6	8 GB	140 GB	5	10 Kerne · 16 GB · 250 GB
10.000	44.000	8	12 GB	160 GB	7	12 Kerne · 16 GB · 300 GB

- Eine **SSD** ist ab etwa 500 Geräten Pflicht, weil jede Messung in die Datenbank geschrieben wird.
- Ab 2.500 Geräten gilt bei mehr Kernen als in der Tabelle: Prüf-Prozesse = Kerne − 1.
- Feste IP-Adresse; während der Installation Internetzugang (Pakete, Python, Node.js).

5.2 Windows Server

Geräte	Prüf-Prozesse	Minimum (CPU · RAM · SSD) und Hinweis
100	0	2 Kerne · 4 GB · 50 GB
500	0	2 Kerne · 4 GB · 70 GB
1.000	0	4 Kerne · 6 GB · 80 GB – Virenscanner-Ausnahme empfohlen
2.500	2	4 Kerne · 8 GB · 100 GB – TCP-Ports/TIME_WAIT anpassen, Virenscanner-Ausnahme
5.000	4	8 Kerne · 12 GB · 140 GB – wie 2.500

Voraussetzungen unter Windows: 64-Bit-Server 2016–2025, freie Ports 80 und 443 (kein IIS darauf), Internet bei der Installation (Python 3.12, Node.js 22) und PowerShell „Als Administrator ausführen“.

6. Installation

6.1 Ubuntu Server 22.04 / 24.04

```
unzip Netoryx-Ubuntu-1.0.1.zip && cd Netoryx-Ubuntu-1.0.1
sudo bash install.sh --domain netoryx.corp.example.at
```

Das Skript installiert in zehn Schritten Systempakete, Dienstbenutzer, Programmdateien, Python-Umgebung, Frontend, systemd-Dienste, nginx mit HTTPS und die Firewall-Regeln. Am Ende erscheinen **Adresse und Startpasswort** – dieses wird nirgends gespeichert und muss bei der ersten Anmeldung geändert werden. Ein erneuter Aufruf von `install.sh` aktualisiert eine bestehende Installation und behält Datenbank, Domain und Zertifikat.

Option	Bedeutung
`--domain <name>`	Hostname der Oberfläche (kommt ins Zertifikat und in die nginx-Konfiguration).
`--tls <modus>`	`self-signed` (Standard), `custom`, `letsencrypt` oder `none`.
`--cert` / `--key`	Eigenes Zertifikat und Schlüssel (PEM) für `--tls custom`.
`--email <adresse>`	Kontakt für Let's Encrypt.
`--dir`, `--data`, `--user`, `--port`	Programmverzeichnis (`/opt/netoryx`), Daten (`/var/lib/netoryx`), Dienstbenutzer, interner API-Port (8000).

6.2 Debian 12 / 13

```
su -                                    # oder: sudo -i
apt install -y unzip
unzip Netoryx-Debian-1.0.1.zip && cd Netoryx-Debian-1.0.1
bash install.sh --domain netoryx.corp.example.at
```

Auf Debian läuft `install.sh` als root auch ohne `sudo`. Das Skript prüft die Debian-Version (Debian 11 ist zu alt), nimmt Node.js aus den signierten Debian-Paketen und installiert bei Bedarf `sudo` und `procps`.

6.3 Docker

```
unzip Netoryx-Docker-1.0.1.zip && cd Netoryx-Docker-1.0.1
cp .env.example .env     # dann NETORYX_DOMAIN und NETORYX_EXTRA_NAMES eintragen
docker compose up -d --build
docker compose logs netoryx   # Adresse und Startpasswort des Admins
```

Das Image wird auf dem Host gebaut (3–8 Minuten). Daten, Zertifikate und Schlüssel liegen in den Volumes `netoryx-data` und `netoryx-config`. Bis etwa 2.500 Geräte reicht `docker-compose.yml` (Bridge-Netz), darüber `docker-compose.host.yml` (Host-Netz) mit den Kernel-Werten aus `docker/99-netoryx-host.conf`. Die CLI öffnet man mit `docker exec -it netoryx netoryx`.

6.4 Windows Server

```
Expand-Archive .\Netoryx-Windows-1.0.1.zip -DestinationPath C:\Temp
cd C:\Temp\Netoryx-Windows-1.0.1
powershell -ExecutionPolicy Bypass -File .\windows\install.ps1 -Domain
netoryx.corp.example.at
```

Das Skript lädt Python 3.12 und Node.js (Signatur bzw. Prüfsumme werden geprüft) und richtet die Dienste **NETORYX** und **NETORYX-Helper** ein. Programmdateien liegen in `C:\Program Files\NETORYX`, Daten und Konfiguration in `C:\ProgramData\NETORYX`. Das CA-Zertifikat für die Clients

gibt es unter `http://<server>/netoryx-ca.crt`; im Domänennetz verteilt man es am einfachsten per GPO.

6.5 Erste Anmeldung und Einrichtung

Eine neue Installation ist **leer**: keine Beispielordner, keine Vorlagen; Active Directory, Single Sign-On, Zwei-Faktor, Duo und E-Mail sind ausgeschaltet.

1. `https://<domain>/` oder `https://<server-ip>/` öffnen.
2. Mit `admin` und dem **Startpasswort** aus der Installationsausgabe anmelden.
3. Der **Einrichtungsassistent** startet: eigenes Passwort festlegen (mindestens 12 Zeichen), Grundeinstellungen (Sprache, Adresse), Datenschutz (Verantwortlicher), Fertig – wahlweise mit Einführungstour.
4. Empfohlen: Zwei-Faktor einschalten, unter *System → Zertifikat* das CA-Zertifikat an die Clients verteilen und Beispielvorlagen unter *Vorlagen* hinzufügen.

> **Notfallzugang**
> Das lokale `admin`-Konto ist der Notfallzugang: Wiederherstellung, Update, Zertifikate und Werkseinstellungen sind nur mit lokalen Administratorkonten möglich – auch wenn später Active Directory, SSO oder Duo genutzt werden.

6.6 Firewall

NETORYX prüft aktiv – eingehend braucht der Server nur den Webzugriff.

Richtung	Protokoll / Port	Wofür
eingehend	TCP 80, 443	Oberfläche (80 leitet auf 443 um und liefert das CA-Zertifikat)
ausgehend	ICMP Echo	PING
ausgehend	UDP 161	SNMP, Systemressourcen
ausgehend	UDP 123	NTP
ausgehend	TCP 5985 / 5986	WinRM (Systemressourcen, Windows-Updates)
ausgehend	TCP 25 / 465 / 587	SMTP-Prüfung und E-Mail-Versand
ausgehend	TCP 80 / 443	HTTP-Prüfung, Webhooks, Single Sign-On
ausgehend	TCP 636 (389)	Active Directory: LDAPS bzw. LDAP mit StartTLS
ausgehend	TCP 443	Duo Security (nur wenn eingeschaltet)
eingehend (Internet)	TCP 80	Nur für Let’s Encrypt (Domainprüfung)
ausgehend	UDP/TCP 53	DNS

7. Bedienung

7.1 Oberfläche

- **Dashboard:** Kennzahlen, Filter und die Liste aller Ausfälle; eigene Dashboards lassen sich aus Bausteinen per Drag & Drop zusammenstellen.

- **Baumansicht:** Ordner, Geräte und je Prüfung eine farbige Kachel – ideal als Übersicht auf einem Monitor.
- **Ereignisse:** alle bestätigten Statuswechsel, filterbar nach UP, WARNING, DOWN und PAUSED.
- **Vorlagen:** Gerätetypen einmal einrichten und beim Anlegen auswählen.
- **Suche (Strg+K):** findet Geräte, Ordner, Dashboards und – für Admins – Benutzer und Einstellungen.
- **Einführungstour:** getrennte Einführung für Admins und Benutzer.

7.2 Prüfungen

Prüfung	Beschreibung
PING	ICMP-Erreichbarkeit; die Antwortzeit ist der Ping-Wert.
TCP	Erreichbarkeit eines TCP-Ports.
HTTP/HTTPS	Abruf einer Seite, z. B. interner Webserver oder Internetseite.
NTP	Antwort eines Zeitservers und Abweichung.
SMTP	Verbindung zu einem Mailserver.
SNMP	Abfrage per SNMP v1/v2c/v3.
Systemressourcen	CPU, RAM, Festplatte, Temperatur und PoE – per SNMP (Profile Cisco, Linux, generisch) oder bei Windows per WinRM.
Windows-Updates	Neustartbedarf, letzte Installation, Installationsfehler – per WinRM, ohne Agent.

7.3 Systemressourcen und Windows-Updates

Auf **Linux** und **Cisco-Geräten** wird per SNMP gelesen; auf den Zielgeräten muss der SNMP-Dienst den NETORYX-Server zulassen (Community bzw. v3-Benutzer, ACL). **Windows-Rechner** werden per WinRM abgefragt – CPU, RAM und alle Laufwerke, ohne SNMP-Dienst. Dafür genügt ein Dienstkonto (z. B. `SVC-…`) ohne Administratorrechte; die nötigen Rechte werden per Gruppe und GPO vergeben. Eine genaue Rechteliste steht in der Anleitung, Kapitel 18.

7.4 Benutzer und Anmeldung

- **Rollen:** Administrator, Lesen & Schreiben, Nur Lesen – mit Ordner-Freigaben inklusive Unterordner.
- **Anmeldung:** lokal, Active Directory/LDAP oder Single Sign-On (OpenID Connect). Rolle und Ordner können aus Gruppenregeln kommen.
- **Zwei-Faktor:** Authenticator-App (Microsoft Authenticator, Google Authenticator …) und/oder Duo Push; die zweite Methode erreicht man über *Andere Anmeldemethode verwenden*.
- **Benutzerdaten:** können heruntergeladen werden (Datenauskunft).

7.5 Benachrichtigungen

E-Mail (über den eingerichteten Mailserver, mit Signatur) und Webhook. Benachrichtigt wird bei UP und bei DOWN; **Regeln** legen fest, für welchen Ordner, Status und welche Risikostufe. Die Benachrichtigung ist pro Gerät einschaltbar und enthält einen Link zur Detailseite.

© 2026 NETORYX – Luca Lindner & Thiemo Hechenblaikner · info@netoryx.at · www.netoryx.at

7.6 Befehlszeile (CLI)

Die CLI bietet alles, was die Oberfläche kann – Geräte (auch viele auf einmal), Prüfungen, Ordner, Vorlagen, Dashboards, Benutzer, Benachrichtigungen, Einstellungen, Sicherungen, Update, Neustart und Zertifikate. Sie öffnet sich im Browser über das Symbol **>_** (Strg+^) oder per SSH: auf dem Server mit dem Befehl `netoryx` (Anmeldung mit dem NETORYX-Konto) oder – optional eingerichtet mit `deploy/ssh-cli.sh on` – direkt über das SSH-Konto `netoryx-cli`. Kontexthilfe gibt es mit `?` wie bei Cisco, zum Beispiel `device ?`.

8. Betrieb und Wartung

8.1 Zertifikate

Unter *System → Zertifikat* stehen drei Wege zur Verfügung: eine **eigene NETORYX-CA** (Standard, Laufzeit einstellbar), **Let's Encrypt** und der **Upload** eines eigenen Zertifikats. Das CA-Zertifikat muss auf den Clients als vertrauenswürdig importiert werden (im Domänennetz per GPO).

8.2 Sicherung und Wiederherstellung

- **Tägliche automatische Sicherungen**, AES-256-verschlüsselt.
- **Block-Level-Deduplizierung:** 14 Sicherungen benötigen nur 15–36 % des Platzes.
- **Aufbewahrung** nach dem Großvater-Vater-Sohn-Prinzip.
- **Download** verschlüsselt (AES-256-ZIP mit Passwort) oder unverschlüsselt.
- **Externer Speicher:** Spiegel auf NAS/Fileserver per SMB; SAN, NFS oder USB als eingehängter Ordner.
- **Wiederherstellung** in der Oberfläche oder auf der Kommandozeile – auch für den Umzug auf einen neuen Server.

8.3 Update, Neustart, Werkseinstellungen

- **Update:** neues Paket unter *System → Update* hochladen (mit Fortschrittsbalken), alternativ erneut `install.sh` bzw. `install.ps1` ausführen. Unter Docker per neuem Image.
- **Neustart:** wahlweise nur NETORYX oder der ganze Server.
- **Werkseinstellungen:** setzen die Installation auf den leeren Zustand zurück – vorher unbedingt eine Sicherung anlegen.
- **Protokolle:** unter *System → Protokolle*; zusätzlich ein Audit-Log.

8.4 Große Installationen

Für bis zu 10.000 Geräte sorgen ein gleichmäßig verteilter Scheduler mit Grenzen je Protokoll, gesammeltes Speichern, Stundenwerte für lange Zeiträume und **Prüf-Prozesse** für mehrere CPU-Kerne. Die Seite *System → Auslastung* zeigt die aktuelle Last; mit `app.cli loadtest` (Docker: `netoryx-manage loadtest`) lässt sich ein Lasttest durchführen.

9. Eigene Prüfungstypen (Plugins)

Das Monitoring ist als **Plugin-System** aufgebaut: eine Datei pro Protokoll. API, Datenbank und Frontend müssen nicht angefasst werden – das Formular im Frontend wird aus der Felddeklaration des Plugins erzeugt.

- Vorhanden sind `ping`, `http`, `ntp`, `snmp`, `smtp`, `tcp`, `resources` und `winupdate`.
- Eigene Plugins werden als `local_<name>.py` im Ordner `backend/app/monitors` gespeichert (z. B. `local_dns.py`). Solche Dateien werden bei Updates **nicht** überschrieben.
- Für SNMP-basierte Plugins eignet sich die Klasse `SnmpSession` aus `_snmp_common.py`; für Windows-Abfragen per PowerShell ist `winupdate.py` die Vorlage.
- Die NETORYX-Lizenz erlaubt eigene Plugins in eigenen Dateien ausdrücklich; die mitgelieferten Dateien selbst dürfen nicht verändert werden.

Ein vollständiges Minimalbeispiel (DNS-Prüfung) steht in der Datei `docs/PROTOKOLLE.md` bzw. im Dokument PROTOKOLLE.

10. Datenschutz, Lizenz und Drittkomponenten

10.1 Datenschutz

NETORYX erhält und sendet **keine Daten an die Entwickler**: kein Cloud-Dienst, keine Telemetrie. Verantwortlich im Sinne der DSGVO ist die Organisation, die NETORYX betreibt. Das Dokument DATENSCHUTZ enthält Vorlagen für das Verzeichnis von Verarbeitungstätigkeiten (Art. 30), technische und organisatorische Maßnahmen (Art. 32), die Umsetzung der Betroffenenrechte, eine Datenschutz-Folgenabschätzung und das Vorgehen bei Datenpannen. Es ist **kein Rechtsrat**.

10.2 NETORYX-Lizenz 1.0

© 2026 NETORYX – Luca Lindner & Thiemo Hechenblaikner. Der Quelltext ist einsehbar, es handelt sich aber nicht um eine Open-Source-Lizenz im Sinne der OSI.

Erlaubt	Nicht erlaubt
Kostenlos nutzen – auch in Unternehmen und gewerblich, als IT-Dienstleister auch in Kundennetzwerken.	NETORYX verändern (Quelltext bearbeiten, Teile übernehmen).
Einrichten über die Einstellungen, offizielle Updates installieren, eigene Plugins (`local_*.py`).	NETORYX verkaufen, vermieten oder gegen Entgelt anbieten (auch als Abo, Gerät oder gehosteter Dienst).
Unverändert und kostenlos weitergeben (mit `LICENSE` und Copyright-Vermerk).	Copyright-Vermerke entfernen oder NETORYX als eigenes Werk ausgeben.
Bezahlte Dienstleistungen rund um NETORYX (Einrichtung, Betreuung, Schulung).	

10.3 Drittkomponenten

NETORYX verwendet Open-Source-Komponenten (u. a. FastAPI, React, pysnmp, icmplib, SQLite). Die Liste samt Lizenzen steht im Dokument THIRD_PARTY_NOTICES.

11. Testumgebung und Testergebnisse

NETORYX wurde in einer eigenen Testumgebung geprüft. Dieses Kapitel zeigt, was getestet wurde, was nur eingeschränkt funktioniert und was noch nicht getestet ist. Getestet wurde Version 1.0.0. Version 1.0.1 ergänzt nur den Sicherungs-Upload (Voll- und Differenzsicherungen, auch als ZIP) und wurde dafür mit den automatischen Tests geprüft.

11.1 Testumgebung

Bereich	Komponenten
VMware-ESXi-Host	Lenovo P510 Workstation
Virtuelle Maschinen	Domain-Controller · WIN11-Client · Ubuntu-Webserver · Mail-Server · NETORYX-Server (Ubuntu)
Cisco-Geräte	Cisco Catalyst Switch · Cisco Access Point (Gen 27)

11.2 Protokolle und Prüfungen

Prüfung	Ergebnis	Status
Ping	Läuft einwandfrei.	**Getestet**
TCP	Läuft einwandfrei.	**Getestet**
HTTP/HTTPS	Funktioniert per HTTP auf dem internen Ubuntu-Webserver und auf der Seite netoryx.at; nicht vollständig umfangreich getestet.	**Teilweise getestet**
NTP	Funktioniert.	**Getestet**
SMTP	Funktioniert mit dem internen Mailserver; nicht vollständig umfangreich getestet.	**Teilweise getestet**
SNMP – Ubuntu Server	CPU, RAM, Speicher und Temperatur funktionieren; die Temperatur nicht immer.	**Getestet**
SNMP – Cisco Catalyst Switch	CPU, RAM, Speicher, PoE-Auslastung pro Port und Temperatur funktionieren.	**Getestet**
SNMP – Cisco Access Point (Gen 27)	Funktioniert nicht. Mögliche Ursache: Der Access Point ist ein Gerät der Generation 27.	**Eingeschränkt**
WinRM – Systemressourcen	Auslesen auf WIN11-Clients ohne Administratorrechte mit einem Dienstkonto (SVC-Account) funktioniert.	**Getestet**
WinRM – Windows-Updates	Nur kurz mit Administratorkonto getestet. Es sollte auch ohne Administratorrechte funktionieren; die Einrichtung per GPO ist in der Anleitung beschrieben.	**Teilweise getestet**

11.3 Oberfläche, Benachrichtigungen und Benutzer

Bereich	Ergebnis	Status
Dashboard	Eigenes Dashboard, Baumansicht, Ereignisse und Vorlagen.	**Getestet**
Benachrichtigungen	Getestet mit dem vorhandenen Mailserver: Mails kommen mit Signatur an – bei UP, bei DOWN und mit Regeln.	**Getestet**
Anmeldung	Lokal, Active-Directory-Login und Single Sign-On.	**Getestet**
Zwei-Faktor	Authenticator-Apps (Microsoft, Google u. a.) und Duo Push.	**Getestet**
Benutzerdaten	Können heruntergeladen werden.	**Getestet**

11.4 Einstellungen und System

Bereich	Ergebnis	Status
Mail-Verbindung	Funktioniert.	**Getestet**
Active Directory	Verbindung getestet mit Windows Server 2025; Rechte über Gruppen getestet.	**Getestet**
Single Sign-On	Verbindung getestet mit Microsoft Entra ID; Rechte über Gruppen getestet.	**Getestet**
Duo Push	Anbindung der Duo-API getestet.	**Getestet**
Audit-Log	Vorhanden und getestet.	**Getestet**
Sicherung (lokal)	Block-Deduplizierung, tägliche automatische Sicherung, AES-256-Verschlüsselung; Download verschlüsselt und unverschlüsselt; Großvater-Vater-Sohn-Prinzip.	**Getestet**
Sicherung auf Fileserver o. Ä.	Externer Speicher (Fileserver, NAS …).	**Nicht getestet**
Zertifikate – eigene CA	Funktioniert.	**Getestet**
Zertifikate – Let's Encrypt	Wurde nicht getestet.	**Nicht getestet**
Zertifikate – PAM	Wurde nicht getestet.	**Nicht getestet**
Update	Über 30 Updates wurden bereits eingespielt.	**Getestet**
Neustart	Beide Varianten (NETORYX und ganzer Server) funktionieren.	**Getestet**
Auslastungsanzeige, Protokolle	Funktionieren.	**Getestet**
Werkseinstellungen	Wurden nicht getestet.	**Nicht getestet**
CLI	Im Browser und per SSH (`netoryx-cli`); Profileinstellungen.	**Getestet**

11.5 Offene Punkte

- Sicherung auf einen externen Speicher (Fileserver, NAS) ist noch **nicht getestet**.
- Zertifikate mit **Let's Encrypt** und **PAM** sind noch **nicht getestet**.
- **Werkseinstellungen** sind noch **nicht getestet** – vor dem ersten Einsatz bitte eine Sicherung anlegen.
- **SNMP-Ressourcen auf dem Cisco Access Point (Gen 27)** funktionieren derzeit nicht.
- **HTTP/HTTPS, SMTP und Windows-Updates** wurden nicht in vollem Umfang getestet.

> **Wichtiger Hinweis zur Funktionsgarantie**
> Wir können nicht garantieren, dass NETORYX in jeder Umgebung zu 100 % fehlerfrei funktioniert.
> Sollten Fehler auftreten, melden Sie diese bitte **so früh wie möglich** – entweder auf der Website im Bereich **Community** oder per E-Mail an **info@netoryx.at**. Wir sehen uns jedes Problem so schnell wie möglich an.

12. Fehler melden und Support

Wir arbeiten laufend an NETORYX. Damit wir Fehler schnell finden und beheben können, sind wir auf Ihre Rückmeldungen angewiesen.

> **Wichtiger Hinweis zur Funktionsgarantie**
> Wir können nicht garantieren, dass NETORYX in jeder Umgebung zu 100 % fehlerfrei funktioniert.
> Sollten Fehler auftreten, melden Sie diese bitte **so früh wie möglich** – entweder auf der Website im Bereich **Community** oder per E-Mail an **info@netoryx.at**. Wir sehen uns jedes Problem so schnell wie möglich an.

12.1 So melden Sie einen Fehler

Kanal	Vorgehen
Website – Community	Beitrag im Bereich **Community** auf der NETORYX-Website erstellen.
E-Mail	Nachricht an **info@netoryx.at** senden.

Bitte nennen Sie in Ihrer Meldung möglichst:

- die **Version** und die **Edition** (Ubuntu, Debian, Docker, Windows) – zu finden in der Datei `VERSION`,
- was Sie getan haben, was Sie erwartet haben und was stattdessen passiert ist,
- betroffene Geräte und Prüfungsarten (z. B. SNMP auf Cisco Access Point),
- Auszüge aus *System → Protokolle* – **ohne Passwörter und Zugangsdaten**,
- gegebenenfalls einen Screenshot.

Anhang: Mitgelieferte Dokumente

Je Edition werden sieben Dokumente auf Deutsch (`_de`) und Englisch (`_en`) als Word-Datei und PDF mitgeliefert. Maßgeblich ist die deutsche Fassung. Ab 1.0.1 liegt außerdem diese NETORYX-Dokumentation in jedem Paket (NETORYX-Dokumentation_de und NETORYX-Documentation_en, als Word-Datei und PDF).

Dokument	Inhalt
README	Überblick, Installation in Kürze, Lizenz.
ANLEITUNG	Vollständige Anleitung mit Inhaltsverzeichnis: Installation, Bedienung, Betrieb, Aufbau.
CHANGELOG	Änderungsprotokoll.
DATENSCHUTZ	Datenschutz (DSGVO/DSG), Urheberrecht, Lizenz, Haftung.
PROTOKOLLE	Protokolle und Prüfmeldungen; eigene Prüfungstypen ergänzen.
THIRD_PARTY_NOTICES	Verwendete Fremdkomponenten und ihre Lizenzen.
LICENSE	NETORYX-Lizenz 1.0.

© 2026 NETORYX – Luca Lindner & Thiemo Hechenblaikner · info@netoryx.at