



NEXUS RMM

— BY HARTMANN74 

Nexus RMM

Installation und Administration

Mit Nexus RMM überwachst und wartest du die Geräte deiner Kunden: Inventar, Patches, Sensoren, Fernwartung, Tickets, Angebote und Rechnungen. Die Software läuft auf deinem eigenen Webserver. Diese Anleitung führt dich von einem leeren Server bis zum ersten überwachten Gerät und zeigt danach die tägliche Administration.

Version 1.0.0.51

Freeware · kostenlos nutzen und unverändert
weitergeben



HARTMANN74
— IT SOLUTIONS —

Inhalt

1 Überblick und Voraussetzungen	4
Was du brauchst	4
2 Server installieren	5
2.1 Pakete installieren	5
2.2 Datenbank anlegen	5
2.3 Dateien auf den Server bringen	5
2.4 Apache einrichten	5
2.5 Web-Installer ausführen	6
3 Erste Einrichtung	9
3.1 Als Plattform-Administrator anmelden	9
3.2 Lizenz eintragen	11
3.3 Ersten Kunden (Mandanten) anlegen	
4 Geräte und Agenten	15
4.1 Gerät anlegen und Installer holen	15
4.2 Windows	19
4.3 Linux	20
4.4 Synology NAS (DSM 7)	
4.5 Windows-EXE bereitstellen (optional, empfohlen)	23
4.6 Das Gerät prüfen	24
5 Täglich mit dem RMM arbeiten	25
5.1 Die Geräteseite	25
5.2 Patches installieren	26
5.3 Konsole und Fernwartung	27
Live-Fernwartung einrichten (einmalig, auf dem Server)	28
Mit der Live-Fernwartung arbeiten	28
Dateimanager	27
5.4 Sensoren und Alarme	30
5.5 Webseiten überwachen	30
5.6 Tickets	31
5.7 Benutzer und Rollen	31
6 Server-Einstellungen	32
6.1 E-Mail über Microsoft 365 (Graph)	
6.2 Automatische Aufgaben (Cron)	
6.3 Zwei-Faktor-Anmeldung	33
6.4 Weitere Einstellungen	34
7 Sicherung und Updates	35

7.1 Sichern	3
7.2 Server aktualisieren	3
7.3 Agenten aktualisieren	3
8 Fehlersuche	3
9 Sicherheit	3

1 Überblick und Voraussetzungen

Nexus RMM besteht aus zwei Teilen: dem **Server** (die Weboberfläche, die du hier installierst) und den **Agenten** (kleine Programme auf den überwachten Geräten). Die Agenten melden sich alle 60 Sekunden beim Server. Der Server baut nie eine Verbindung zu den Geräten auf. Auf den Geräten muss deshalb kein Port geöffnet werden.

Was du brauchst

- Einen Linux-Webserver (Ubuntu 22.04/24.04 oder Debian 12) mit Root- oder sudo-Zugriff, oder ein Webhosting-Paket mit PHP und MariaDB
- Apache 2.4 mit den Modulen `rewrite` und `headers`
- PHP 8.1 oder neuer mit den Erweiterungen pdo_mysql, openssl, zip, mbstring, curl, gd (sodium wird für die Lizenzprüfung empfohlen)
- MariaDB 10.5 oder neuer (oder MySQL 8)
- Eine eigene Domain oder Subdomain mit HTTPS, zum Beispiel `rmm.deine-firma.de`
- Deinen Lizenzschlüssel (kommt nach dem Kauf per E-Mail) und das Programmpaket (ZIP) aus deinem Kundenkonto
- Für die Agenten: Windows 10/11 oder Server 2016+, Linux mit systemd und Python 3, oder Synology DSM 7 mit Python 3

Tipp

Plane etwa 15 Minuten für die Server-Installation ein. Die Agenten sind danach in jeweils unter einer Minute installiert.

2 Server installieren

2.1 Pakete installieren

Auf Ubuntu oder Debian als Administrator:

```
sudo apt update
sudo apt install apache2 mariadb-server php php-mysql php-zip php-mbstring \
    php-curl php-gd php-xml libapache2-mod-php unzip
sudo a2enmod rewrite headers
sudo systemctl restart apache2
```

2.2 Datenbank anlegen

```
sudo mysql
CREATE DATABASE nexusrmm CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'nexusrmm'@'localhost' IDENTIFIED BY 'EIN-STARKES-PASSWORT';
GRANT ALL PRIVILEGES ON nexusrmm.* TO 'nexusrmm'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

Notiere Datenbankname, Benutzer und Passwort. Du brauchst sie gleich im Installer. Verwende nicht den Datenbank-Benutzer `root`.

2.3 Dateien auf den Server bringen

1. Kopiere das ZIP auf den Server (zum Beispiel mit SFTP nach `/tmp`).
2. Entpacke es und verschiebe den Inhalt in das Webverzeichnis der Domain. Wichtig: Auch die versteckten Dateien `.htaccess` und `.user.ini` müssen mitkommen.
3. Setze die Rechte. Der Webserver-Benutzer heißt unter Ubuntu `www-data`.

```
cd /tmp && unzip -q hartmann74-nexusrmm-*.zip
sudo mkdir -p /var/www/rmm
sudo cp -a nexus-rmm/. /var/www/rmm/
sudo chown -R www-data:www-data /var/www/rmm
sudo chmod -R u+rwX /var/www/rmm
```

Hinweis

Heißt der entpackte Ordner bei dir anders, passe den Namen im Befehl an. Entscheidend ist, dass `index.php`, `install.php` und `.htaccess` direkt in `/var/www/rmm` liegen.

2.4 Apache einrichten

Lege die Datei `/etc/apache2/sites-available/rmm.conf` an:

```
<VirtualHost *:80>
    ServerName rmm.deine-firma.de
    DocumentRoot /var/www/rmm
    <Directory /var/www/rmm>
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

Seite aktivieren und kostenloses HTTPS-Zertifikat von Let's Encrypt holen:

```
sudo a2ensite rmm
sudo systemctl reload apache2
sudo apt install certbot python3-certbot-apache
sudo certbot --apache -d rmm.deine-firma.de
```

Wichtig

`AllowOverride All` ist Pflicht. Ohne diese Einstellung funktionieren die Adressen der Seite nicht, und die Programm-Ordner sind nicht geschützt. Betreibe das RMM ausschließlich über HTTPS: Die Agenten übertragen ihren Schlüssel bei jeder Meldung.

2.5 Web-Installer ausführen

Öffne `https://rmm.deine-firma.de/install.php`. Trage ein:

Hartmann74 Inventory Pro – Einrichtung

Datenbank (MariaDB/MySQL)

Host

localhost

Port

3306

1

Datenbank-Benutzer

nexusrmm

Datenbank-Passwort

Jedes Zeichen ist erlaubt, auch # @ % / usw. – wird nicht in eine URL eingebaut.

2

Datenbankname

nexusrmm

Öffentliche Adresse

3

Basis-URL (ohne / am Ende)

https://rmm.deine-firma.de

Erster Plattform-Zugang (Superadmin)

Damit meldest du dich unter /superadmin/login an, um danach Kunden (Mandanten) anzulegen. Wird nur angelegt, falls noch kein Superadmin existiert.

4

Benutzername

admin

5

Passwort (mind. 6 Zeichen)

Passwort wiederholen

Einrichten

Der Web-Installer. Die roten Nummern gehören zur Liste darunter.

- 1 Datenbank-Benutzer** und Passwort aus Schritt 2.2. Host ist meist `localhost`, Port `3306`.
- 2 Datenbankname** aus Schritt 2.2.
- 3 Öffentliche Adresse** mit `https://` und ohne Schrägstrich am Ende. Die Agenten bekommen diese Adresse als Ziel.
- 4 Benutzername des Plattform-Administrators** (Superadmin).
- 5 Passwort des Superadmins.** Der Installer verlangt mindestens 6 Zeichen. Wähle mindestens 12 und wiederhole es im Feld darunter.

Klicke auf **Einrichten**. Der Installer legt die Tabellen und die Datei `config.php` an.

Hartmann74 Inventory Pro – Einrichtung

Fertig! Die App ist eingerichtet, die Datenbank-Tabellen wurden angelegt.

1

Jetzt als Superadmin anmelden

Aus Sicherheitsgründen kann diese Seite jetzt nicht mehr ausgeführt werden, ohne zuerst `config.php` zu löschen. Als nächstes: im Superadmin-Bereich einen Kunden (Mandanten) anlegen, danach kann sich dieser unter `/t/<kennung>/login` anmelden.

Meldung nach erfolgreicher Einrichtung.

- 1 Mit diesem Link gelangst du zur Anmeldung des Plattform-Administrators.

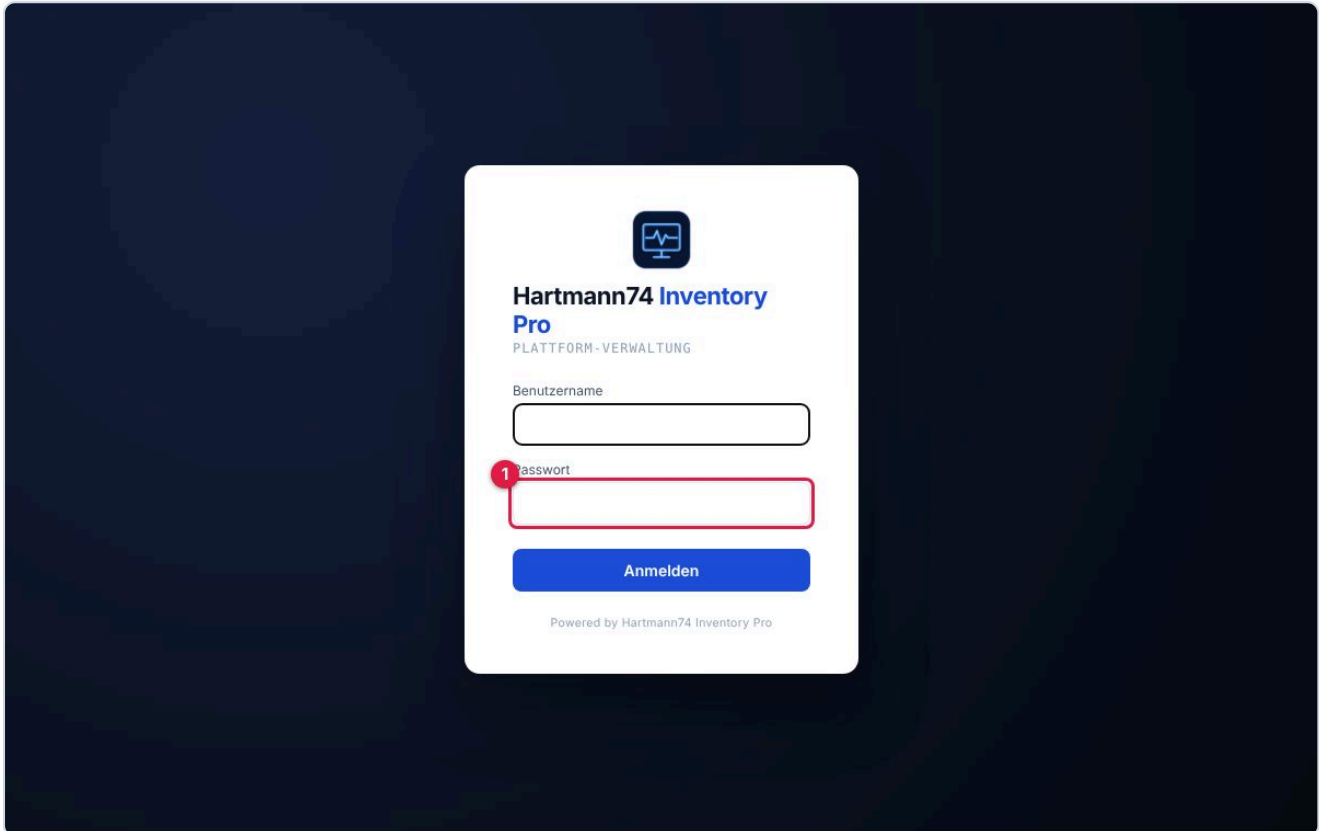
Wichtig

Lösche jetzt `install.php`: `sudo rm /var/www/rmm/install.php`. Sichere außerdem `config.php` und `data/secret.key` an einem Ort außerhalb des Webverzeichnis. Mit dem Schlüssel sind die gespeicherten Passwörter verschlüsselt. Geht er verloren, sind sie nicht mehr lesbar.

3 Erste Einrichtung

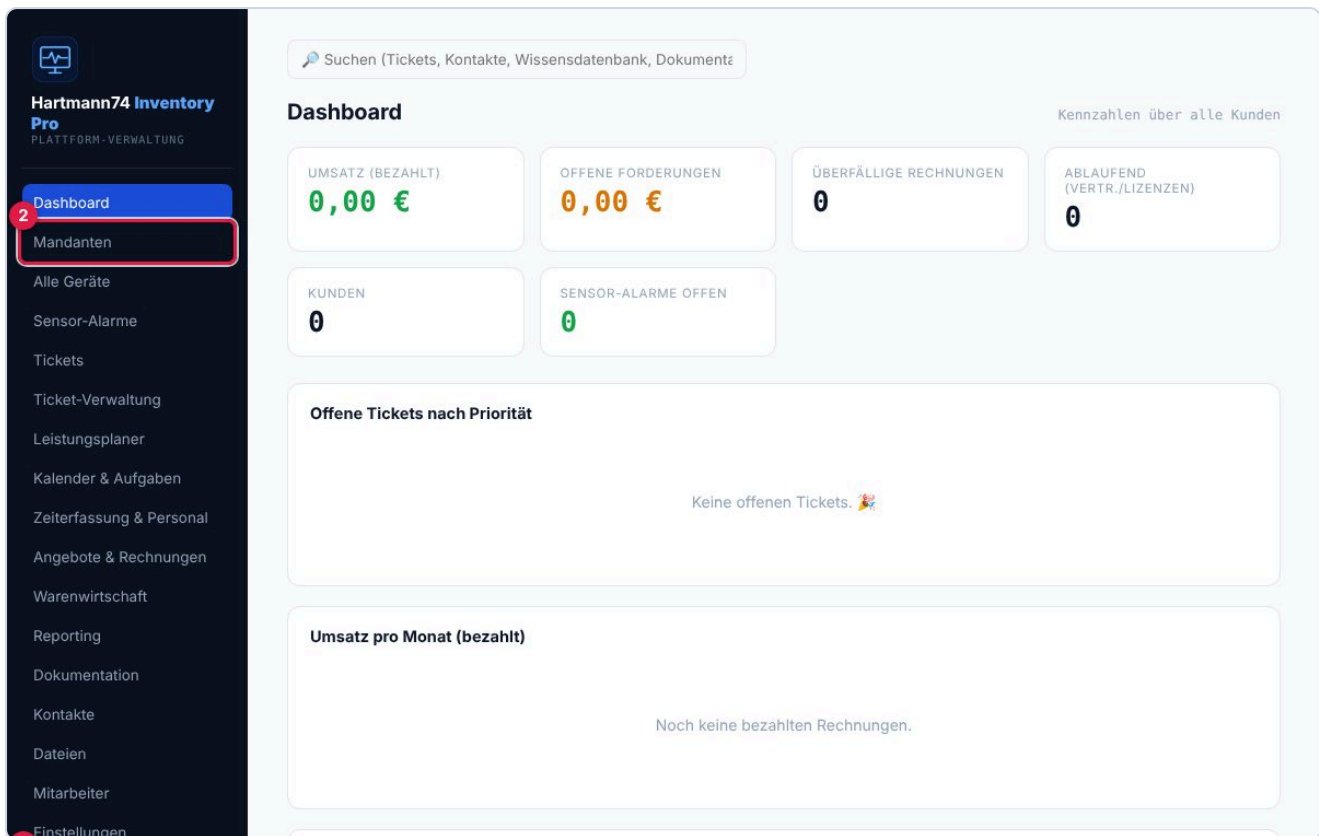
3.1 Als Plattform-Administrator anmelden

Öffne <https://rmm.deine-firma.de/superadmin/login> und melde dich mit dem Superadmin aus dem Installer an. Die Plattform-Verwaltung ist dein Bereich. Sie ist unabhängig von den Kunden (Mandanten), die du später anlegst.



Anmeldung des Plattform-Administrators.

- 1 Passwort-Feld. Benutzername steht darüber.



Die Plattform-Verwaltung mit der Menüleiste links.

- 1 **Mandanten:** deine Kunden anlegen und verwalten.
- 2 **Lizenz:** Lizenzschlüssel eintragen.
- 3 **System-Update:** neue Programmversionen einspielen.

3.2 Lizenz eintragen

Hartmann74 Inventory Pro
PLATTFORM-VERWALTUNG

Suchen (Tickets, Kontakte, Wissensdatenbank, Dokumente)

Lizenz Lizenzschlüssel eintragen und Status prüfen

Status: **Nicht gültig**
Keine Lizenz hinterlegt

Lizenzschlüssel hinterlegen

1 H74LIC1....

2 **Speichern**

Die Lizenzseite vor dem Eintragen.

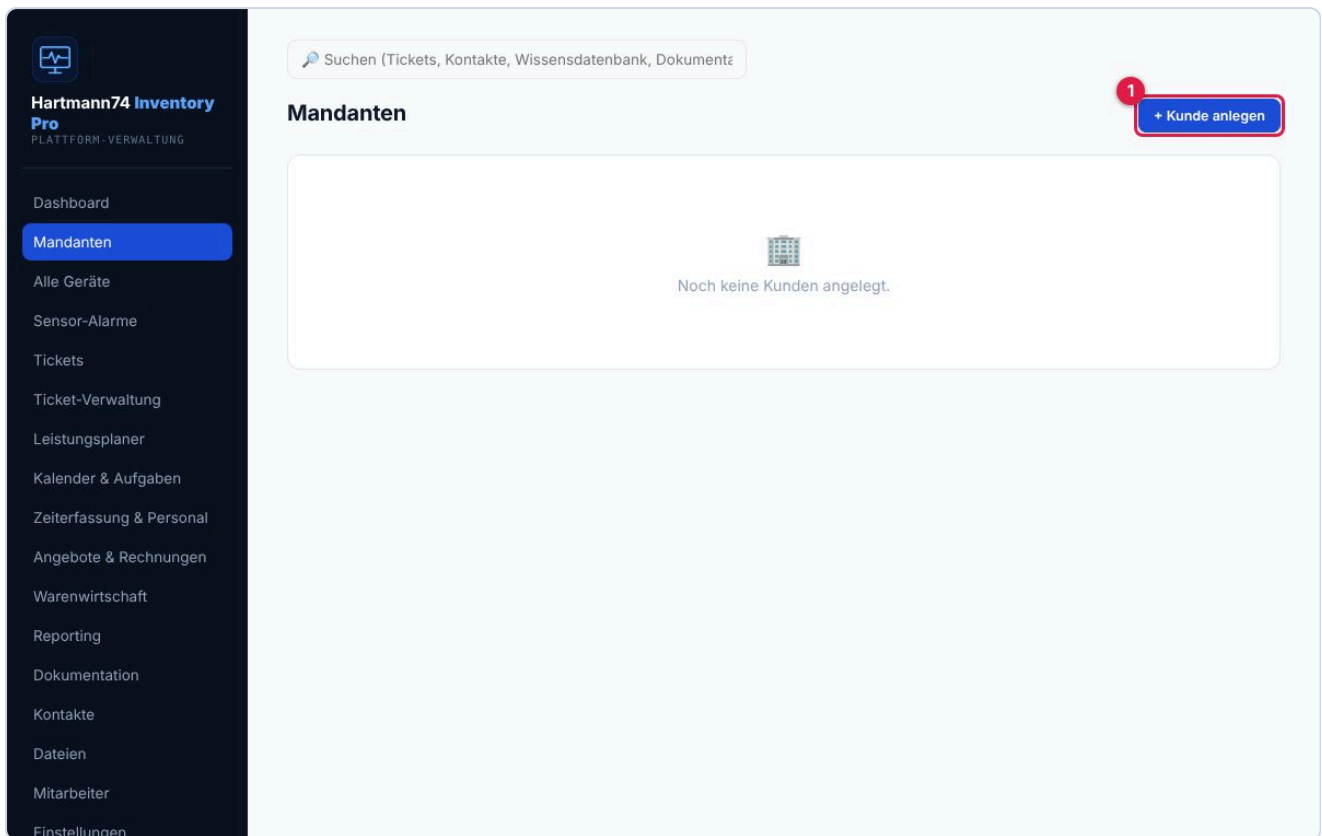
- 1 Lizenzschlüssel einfügen. Er beginnt mit **H74LIC1.** und ist eine lange Zeichenfolge. Kopiere ihn komplett und ohne Leerzeichen.
- 2 **Speichern** klicken. Der Status wechselt auf „gültig“ und zeigt, wie viele Kunden du anlegen darfst.

Hinweis

Ohne gültige Lizenz sind die Kunden-Bereiche gesperrt. Die Plattform-Verwaltung bleibt immer erreichbar, damit du die Lizenz eintragen kannst.

3.3 Ersten Kunden (Mandanten) anlegen

Jeder Kunde bekommt einen eigenen, abgeschotteten Bereich mit eigener Anmeldeadresse, eigenen Geräten, Tickets und Benutzern.



Mandantenliste vor dem ersten Kunden.

- 1 Auf **+ Kunde anlegen** klicken.

Hartmann74 Inventory Pro
PLATTFORM-VERWALTUNG

Suchen (Tickets, Kontakte, Wissensdatenbank, Dokumente)

Neuen Kunden anlegen

1 Firmenname
Musterfirma GmbH

2 Login-Kennung (Teil der URL)
musterfirma-gmbh

3 Erster Admin-Benutzername
admin

4 Erstes Admin-Passwort (mind. 6 Zeichen)
Sehr-Sicheres-Passwort-2026

Firmenfarbe
Logo (optional, PNG/JPG/SVG, max. 2 MB)
Choose File No file chosen

5 Abbrechen Anlegen

Dialog „Neuen Kunden anlegen“.

- 1 **Firmenname** des Kunden.
- 2 **Login-Kennung**. Sie wird Teil der Anmeldeadresse und aus dem Namen vorgeschlagen.
- 3 **Erster Admin-Benutzername** des Kunden.
- 4 **Erstes Admin-Passwort**. Der Kunde sollte es nach der ersten Anmeldung ändern.
- 5 **Anlegen** klicken. Optional kannst du vorher Firmenfarbe und Logo des Kunden einstellen.

**Hartmann74 Inventory Pro**
PLATTFORM-VERWALTUNG

Dashboard

Mandanten

Alle Geräte

Sensor-Alarme

Tickets

Ticket-Verwaltung

Leistungsplaner

Kalender & Aufgaben

Zeiterfassung & Personal

Angebote & Rechnungen

Warenwirtschaft

Reporting

Dokumentation

Kontakte

Dateien

Mitarbeiter

Einstellungen

Suchen (Tickets, Kontakte, Wissensdatenbank, Dokumente)

Mandanten

+ Kunde anlegen

NAME	LOGIN-LINK	GERÄTE	BENUTZER	FARBE	
— Musterfirma GmbH	http://127.0.0.1:8201/t/musterfirma-gmbh/login	0	1		Öffnen Bearbeiten Löschen

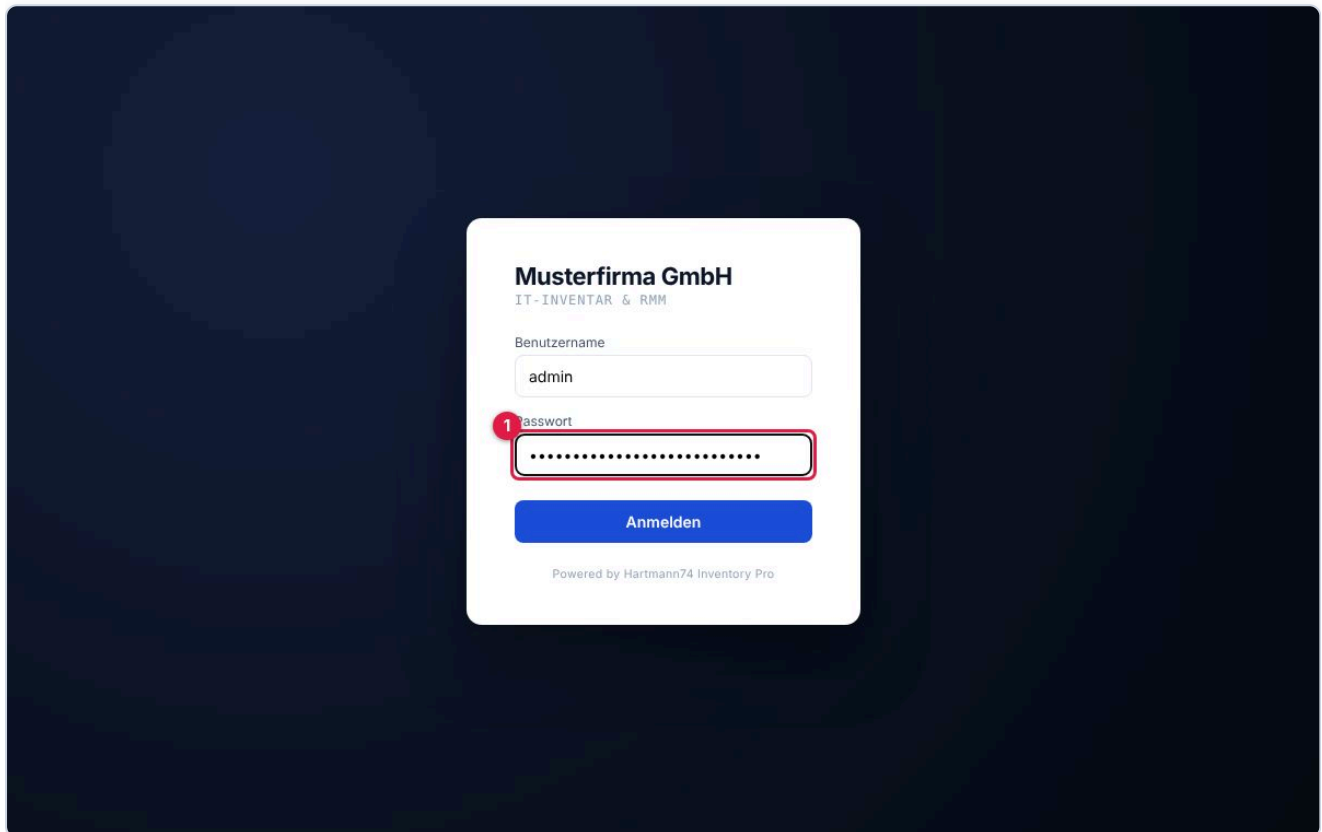
Der angelegte Kunde in der Mandantenliste.

- 1 Anmeldeadresse des Kunden. Gib sie dem Kunden weiter: `https://rmm.deine-firma.de/t/<kennung>/login`.
- 2 **Öffnen** wechselt direkt in den Bereich des Kunden.

4 Geräte und Agenten

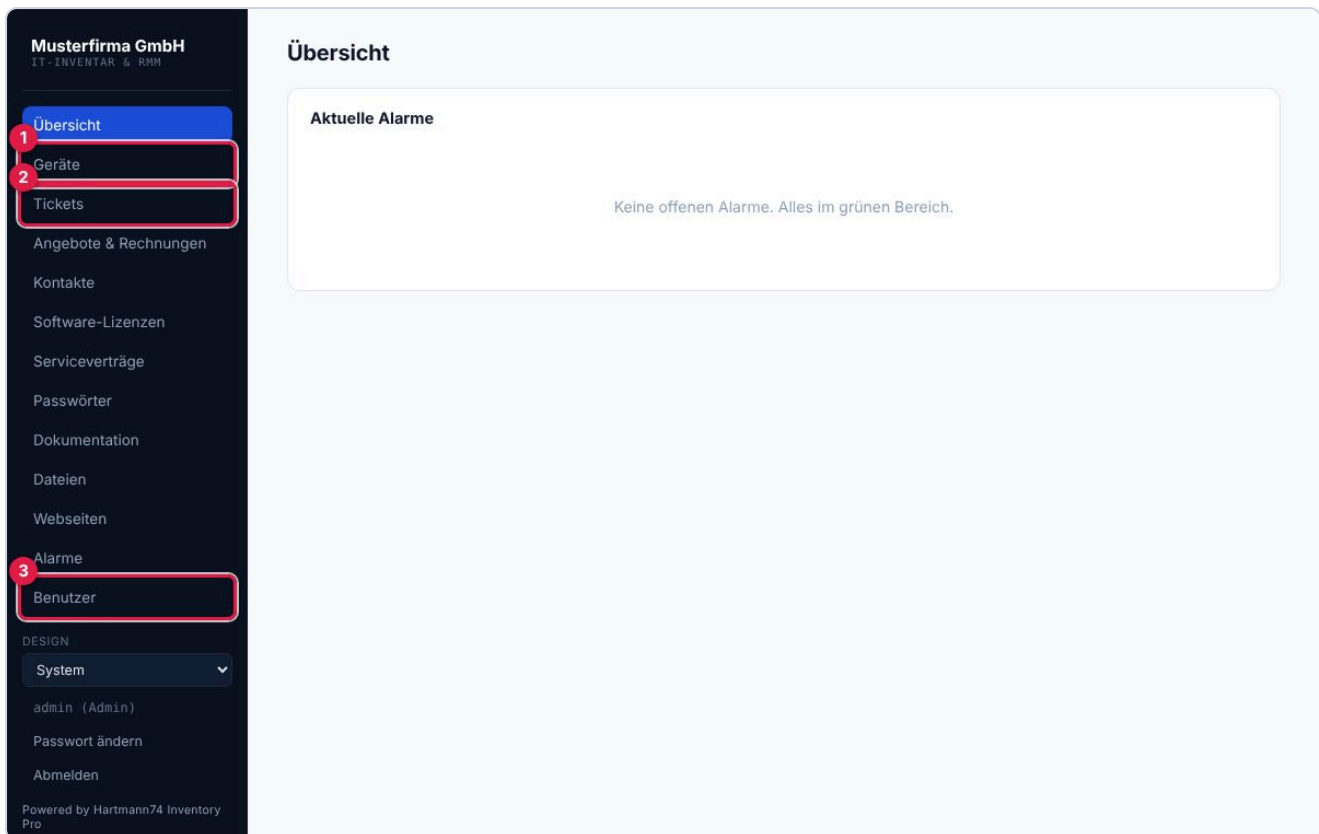
Ein Gerät wird immer in zwei Schritten verbunden: Du legst es beim Kunden an. Dabei entsteht ein persönlicher Agent-Schlüssel. Dann installierst du den Agenten auf dem Gerät. Sobald er sich meldet, erscheint das Gerät als „online“.

4.1 Gerät anlegen und Installer holen



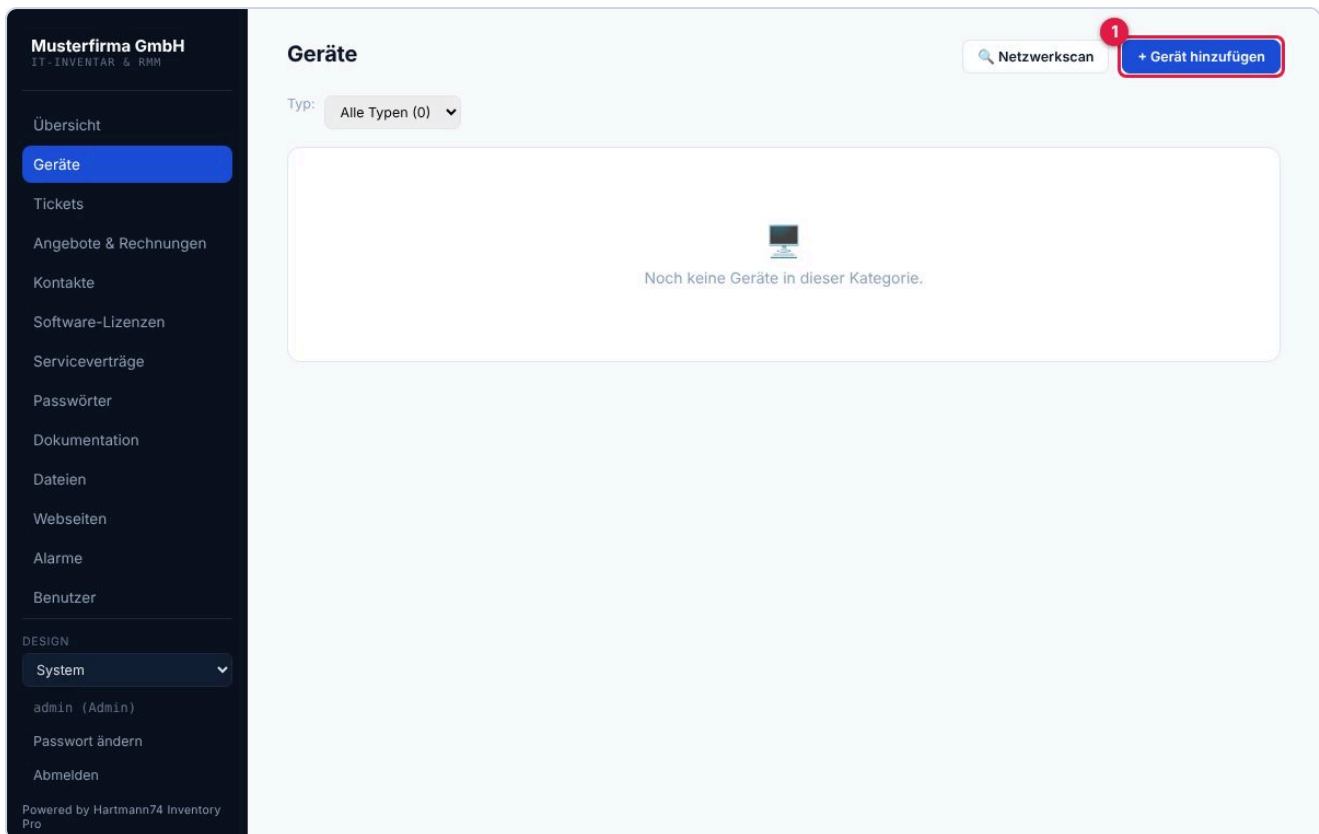
Anmeldung im Bereich des Kunden.

- 1 Anmelden mit dem Admin des Kunden.



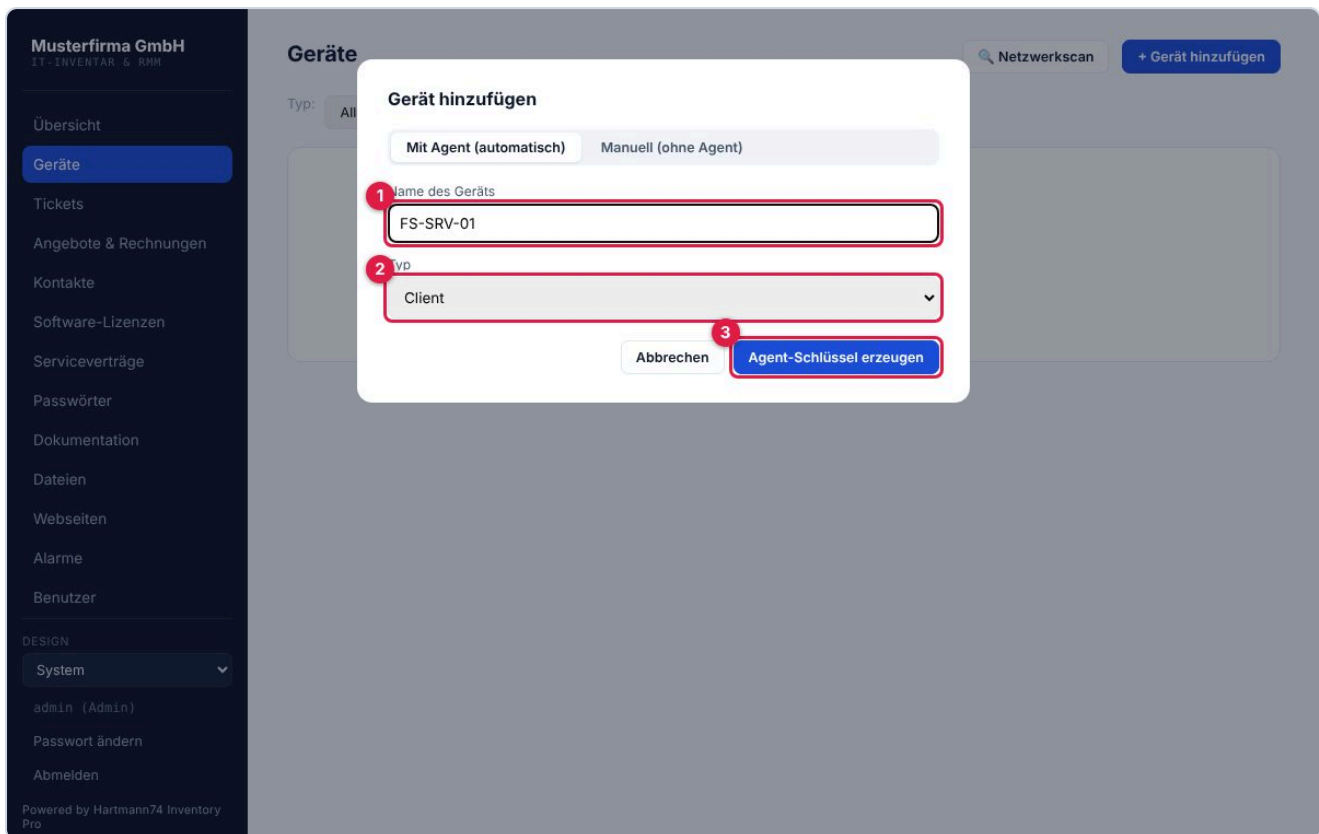
Übersicht im Kundenbereich.

- 1 **Geräte:** hier legst du Geräte an.
- 2 **Tickets:** Support-Tickets des Kunden.
- 3 **Benutzer:** weitere Mitarbeiter des Kunden anlegen.



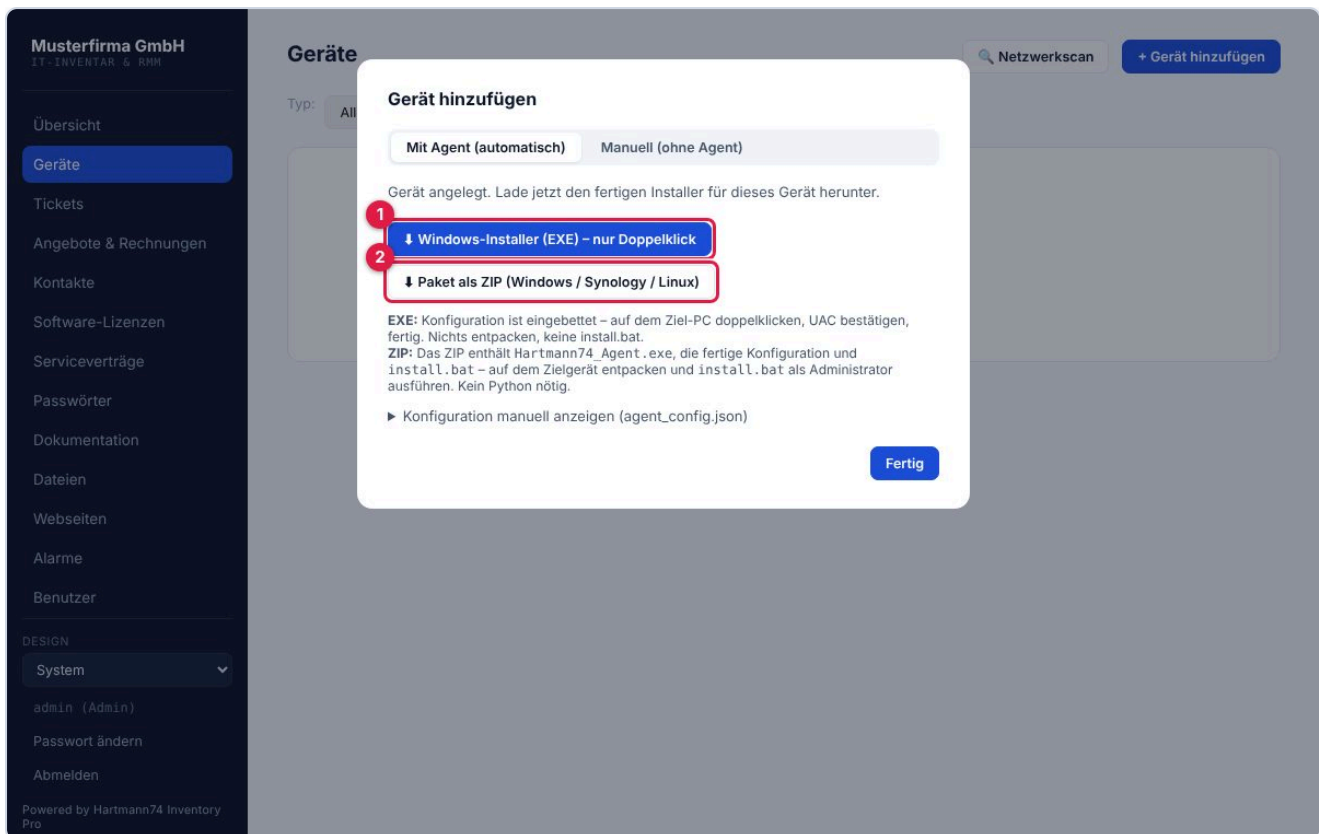
Geräteliste vor dem ersten Gerät.

1 + Gerät hinzufügen klicken.



Dialog „Gerät hinzufügen“, Reiter „Mit Agent“.

- 1 **Name des Geräts**, zum Beispiel `FS-SRV-01`.
- 2 **Typ** wählen (Server, Client, NAS, Firewall, Router, Switch, Access Point, Drucker, USV, Kamera, Telefon oder Sonstige).
- 3 **Agent-Schlüssel erzeugen** klicken.



Der Installer für dieses Gerät.

- 1 **Windows-Installer (EXE):** Doppelklick genügt. Die Konfiguration ist eingebettet.
- 2 **Paket als ZIP:** für Windows, Linux und Synology oder wenn keine EXE bereitliegt.

Hinweis

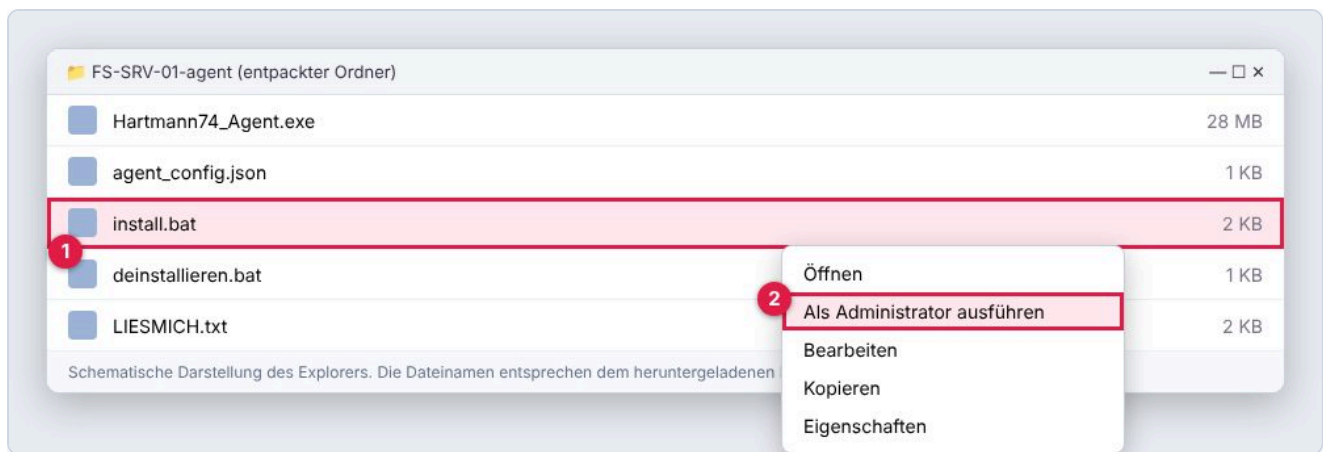
Die EXE-Schaltfläche erscheint nur, wenn auf dem Server die Datei `agent_dist/Hartmann74_Agent.exe` liegt. Wie du sie bereitstellst, steht in Abschnitt 4.5. Das ZIP funktioniert immer.

Wichtig

Der Agent-Schlüssel ist wie ein Passwort: Wer ihn hat, kann in seinem Namen Meldungen senden und Befehle ausführen lassen. Gib das ZIP nicht weiter, versende es nicht per E-Mail und lösche es nach der Installation.

4.2 Windows

1. Lade die EXE (oder das ZIP) auf dem Windows-Gerät herunter. Beim ZIP: entpacken.
2. **EXE:** Doppelklick und die Rückfrage der Benutzerkontensteuerung bestätigen. **ZIP:** Rechtsklick auf `install.bat` → „Als Administrator ausführen“.
3. Warte auf die Meldung „Fertig“. Das Gerät erscheint innerhalb einer Minute im Dashboard als online.



So startest du `install.bat` aus dem ZIP.

- 1 `install.bat` markieren und Rechtsklick.
- 2 „Als Administrator ausführen“ wählen.



Ausgabe von `install.bat` bei erfolgreicher Installation.

Was `install.bat` macht: Es kopiert den Agenten nach `C:\ProgramData\Hartmann74\Agent`, beschränkt den Zugriff auf SYSTEM und Administratoren, führt einen Test-Check-in aus und legt in der Aufgabenplanung die Aufgabe „Hartmann74 Agent“ an (Start beim Systemstart, als SYSTEM). Zum Entfernen führst du `deinstallieren.bat` als Administrator aus.

Hinweis

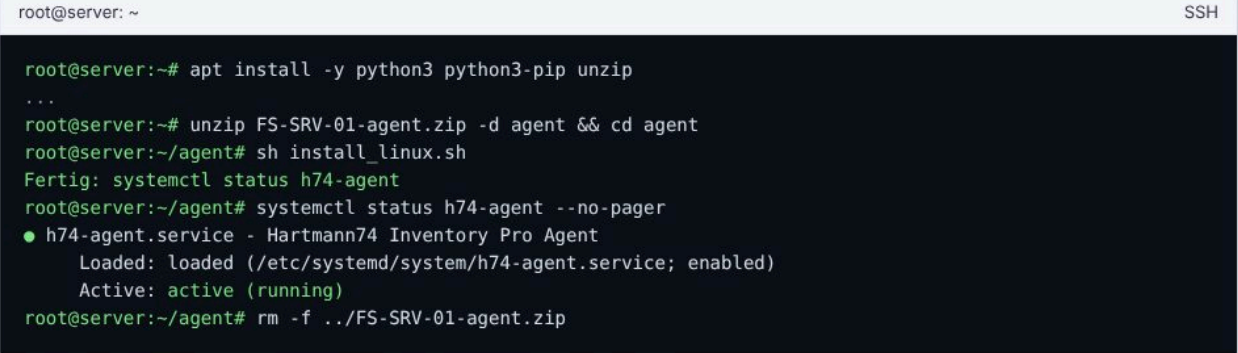
Wird das Paket ohne EXE erzeugt, braucht der PC Python 3 (python.org, beim Setup „Add python.exe to PATH“ anhängen). `install.bat` installiert dann `requests` und `psutil` selbst.

4.3 Linux

Voraussetzung: systemd und Python 3. Als root:

```
apt install -y python3 python3-pip unzip
unzip FS-SRV-01-agent.zip -d agent && cd agent
sh install_linux.sh
```

Das Skript kopiert den Agenten nach `/opt/h74agent`, installiert `requests` und `psutil`, führt einen Test-Check-in aus und richtet den Dienst `h74-agent` ein, der beim Start automatisch läuft.



```
root@server: ~ SSH

root@server:~# apt install -y python3 python3-pip unzip
...
root@server:~# unzip FS-SRV-01-agent.zip -d agent && cd agent
root@server:~/agent# sh install_linux.sh
Fertig: systemctl status h74-agent
root@server:~/agent# systemctl status h74-agent --no-pager
● h74-agent.service - Hartmann74 Inventory Pro Agent
   Loaded: loaded (/etc/systemd/system/h74-agent.service; enabled)
   Active: active (running)
root@server:~/agent# rm -f ../FS-SRV-01-agent.zip
```

Beispielausgabe (Ubuntu). Die Meldungen von apt/pip können je nach Server abweichen.

Installation und Kontrolle auf einem Linux-Server.

Dienst prüfen und Protokoll ansehen:

```
systemctl status h74-agent
journalctl -u h74-agent -n 50 --no-pager
```

Hinweis

Neuere Ubuntu-Versionen verweigern `pip install` ohne Zusatz. Das Skript versucht es zuerst normal. Meldet es einen Fehler, installiere die Module mit `apt install python3-requests python3-psutil` und starte `install_linux.sh` erneut.

4.4 Synology NAS (DSM 7)

Auf dem NAS wird der Agent über die Aufgabenplanung installiert. Du brauchst kein SSH. Voraussetzung ist das Paket **Python 3** (Paketzentrum) und Internetzugang des NAS.

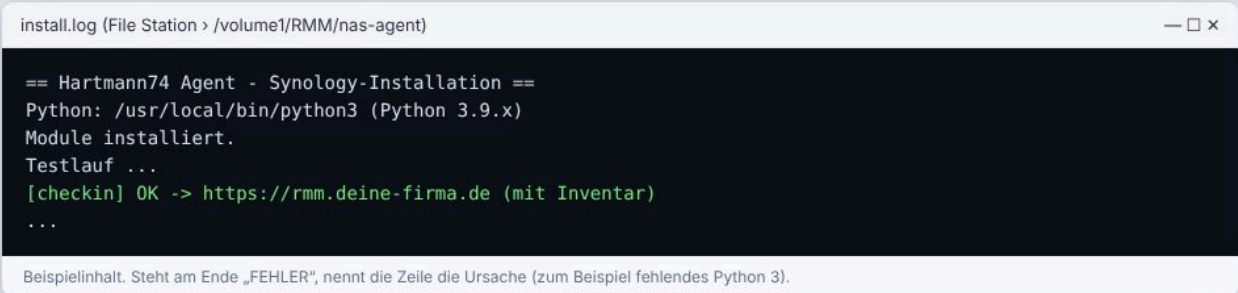
1. Lege in der File Station einen Ordner `RMM/nas-agent` an (Pfad `/volume1/RMM/nas-agent`).
2. Entpacke das ZIP auf deinem PC und lade `h74_agent.py`, `agent_config.json` und `install_synology.sh` in diesen Ordner hoch. Lade auch `h74_inventory.py` und `h74_netscan.py` hoch, falls sie im ZIP liegen.
3. Öffne **Systemsteuerung** → **Aufgabenplaner** → **Erstellen** → **Geplante Aufgabe** → **Benutzerdefiniertes Skript**.
4. Reiter **Allgemein**: Name `Hartmann74 Agent installieren`, Benutzer `root`. Reiter **Zeitplan**: „Am folgenden Datum“ (einmalig). Reiter **Aufgabeneinstellungen**: Befehl `sh /volume1/RMM/nas-agent/install_synology.sh`.
5. Aufgabe markieren und auf **Ausführen** klicken. Nach etwa einer Minute steht das Ergebnis in `/volume1/RMM/nas-agent/install.log`.
6. Lege eine zweite Aufgabe an: **Erstellen** → **Ausgelöste Aufgabe** → **Benutzerdefiniertes Skript**. Ereignis `Hochfahren`, Benutzer `root`, Befehl `sh /volume1/RMM/nas-agent/start.sh`. Sie startet

den Agenten bei jedem Neustart des NAS.

7. Führe die zweite Aufgabe einmal manuell aus. Das NAS erscheint danach als online.

Die einmalige Installationsaufgabe.

- 1 Befehl im Reiter „Aufgabeneinstellungen“.
- 2 Benutzer `root` im Reiter „Allgemein“.



```
install.log (File Station > /volume1/RMM/nas-agent)

== Hartmann74 Agent - Synology-Installation ==
Python: /usr/local/bin/python3 (Python 3.9.x)
Module installiert.
Testlauf ...
[checkin] OK -> https://rmm.deine-firma.de (mit Inventar)
...
```

Das Installationsprotokoll `install.log`.

Erstellen > Ausgelöste Aufgabe > Benutzerdefiniertes Skript

Allgemein Aufgabeneinstellungen

① Ereignis
Hochfahren

② Benutzer
root

③ Befehl ausführen
sh /volume1/RMM/nas-agent/start.sh

Schematische Darstellung (DSM 7). Die Aufgabe startet den Agenten bei jedem Neustart des NAS.

Die Aufgabe für den Autostart.

- 1 Ereignis „Hochfahren“.
- 2 Benutzer `root`.
- 3 Befehl `sh /volume1/RMM/nas-agent/start.sh`.

Hinweis

Steht im Protokoll „Kein python3 gefunden“, installiere im Paketzentrum das Paket „Python 3“. Steht dort „pip install fehlgeschlagen“, prüfe den Internetzugang des NAS.

4.5 Windows-EXE bereitstellen (optional, empfohlen)

Die EXE ist ein einzelnes Programm mit allem Nötigen. Auf dem Zielgerät muss kein Python installiert sein. Liegt `agent_dist/Hartmann74_Agent.exe` im Webverzeichnis, bietet der Dialog „Gerät hinzufügen“ den Windows-Installer an.

Falls die EXE nicht im Paket liegt, baust du sie einmal selbst auf einem Windows-PC:

1. Installiere Python 3.10 oder neuer (python.org, „Add to PATH“ anhängen).
2. Öffne eine Eingabeaufforderung und führe aus: `pip install pyinstaller requests psutil mss pillow`
3. Kopiere den Ordner `agent` und `desktop` des Programmpakets auf den PC und starte `desktop\build_agent_exe.bat`.
4. Kopiere `Hartmann74_Agent.exe` und `agent_version.txt` aus dem entstandenen Ordner `agent_dist` auf den Server nach `/var/www/rmm/agent_dist/`.

Tipp

Spätere Programmänderungen am Agenten brauchen keine neue EXE: Der Server liefert neuen Agent-Code an die laufenden Agenten, die ihn selbst einspielen. Nur wenn eine neue Programmbibliothek nötig wird, bauen wir dir eine neue EXE mit.

4.6 Das Gerät prüfen

Musterfirma GmbH
IT-INVENTAR & RMM

Übersicht
Geräte
Tickets
Angebote & Rechnungen
Kontakte
Software-Lizenzen
Serviceverträge
Passwörter
Dokumentation
Dateien
Webseiten
Alarmer 2
Benutzer

DESIGN
System
admin (Admin)
Passwort ändern
Abmelden
Powered by Hartmann74 Inventory Pro

Geräte

Typ: Alle Typen (1) ▼

Netzwerkscan + Gerät hinzufügen

	NAME	TYP	HERSTELLER / MODELL	BETRIEBSSYSTEM	IP-ADRESSE	LETZTER CHECK-IN
1	FS-SRV-01	Client	—	Linux	192.0.2.2	09.10.2026, 15:55

Das Gerät erscheint in der Geräteliste mit grünem Punkt.

1 Name des Geräts. Klick öffnet die Detailseite.

Meldet sich das Gerät nicht innerhalb von zwei Minuten, hilft die Fehlersuche in Abschnitt 8.

5 Täglich mit dem RMM arbeiten

5.1 Die Geräteseite

The screenshot shows the RMM interface for a device named FS-SRV-01. The sidebar on the left contains navigation links: Übersicht, Geräte (highlighted), Tickets, Angebote & Rechnungen, Kontakte, Software-Lizenzen, Serviceverträge, Passwörter, Dokumentation, Dateien, Webseiten, Alarmer (2), Benutzer, and a DESIGN dropdown menu with System selected. The main content area has a top bar with links: Zurück, QR-Code / Etikett, Hardware-Doku (PDF), Agent-Installer (EXE) (highlighted with a red circle 2), ZIP, and Bearbeiten. Below this, the device status is shown as Online (highlighted with a red circle 1). Other metrics include: LETZTER CHECK-IN (09.10.2026, 15:55), AGENT-VERSION (1.0.0.48), UPTIME (1h), NEUSTART AUSSTEHEND (Nein), PATCHES OFFEN (28), and VOLUMES < 10 % FREI (2). A section for VIRENSCHUTZ and FEHLER (24 H) shows 0 errors. Below this is a tabbed interface with tabs: Übersicht, Sensoren, Tickets (0), Dokumentation (0), Datenträger (9), Netzwerk (3), Hardware, Software (500), and Patches (28) (highlighted with a red circle 3). The 'Fernwartung & Konsole' tab is also highlighted with a red circle 4. The 'Systeminformationen' section displays a table of system details: TYP (client), OS-VERSION / BUILD (24.04), LETZTER NEUSTART (09.10.2026, 17:22), ANGEMELDETER BENUTZER (—), MODELL (—), MAC-ADRESSE (e6:ab:c0:a0:6e:99), SYSTEMLAUFWERK FREI (23 / 252 GB), INVENTAR-STAND (09.10.2026, 15:55), HOSTNAME (vm), ARCHITEKTUR (x86_64), UPTIME (1h), ZEITZONE (Etc/UTC), SERIENNUMMER (—), CPU (Intel(R) Xeon(R) Processor @ 2.80GHz), STANDORT (—), NOTIZEN (—), BETRIEBSSYSTEM (Ubuntu 24.04.5 LTS), INSTALLIERT AM (—), DOMÄNE / ARBEITSGRUPPE (vm), HERSTELLER (—), IP-ADRESSE (192.0.2.2), RAM (7.8 GB), and SERVICEVERTRAG (—).

Detailseite eines Geräts.

- 1 Status: **Online** heißt, der letzte Check-in liegt weniger als zwei Minuten zurück.
- 2 **Agent-Installer (EXE)** und **ZIP** erzeugen den Installer für dieses Gerät erneut.
- 3 **Patches**: ausstehende Updates mit Anzahl.
- 4 **Fernwartung & Konsole**: Shell auf dem Gerät.

Die Reiter im Überblick:

Reiter	Inhalt
Übersicht	Betriebssystem, Hostname, Uptime, Domäne, CPU, RAM, Netzwerk, Seriennummer, Hersteller
Sensoren	Auslastung im Verlauf (24 Std., 7 Tage, 30 Tage) und Schwellwerte für Speicherplatz, Arbeitsspeicher, CPU und Netzwerk
Tickets / Dokumentation	Tickets und Wissensartikel zu diesem Gerät
Datenträger / Netzwerk / Hardware	Laufwerke mit Belegung, Netzwerkkarten, Hardware-Details

Software	Installierte Programme
Patches	Ausstehende Updates, einzeln installierbar
Dienste / Prozesse	Laufende Dienste und Prozesse
Sicherheit & Benutzer	Virenschutz, Firewall, angemeldete Benutzer
Ereignisse	Auffällige Einträge aus dem Ereignisprotokoll
Felder	Eigene Zusatzfelder, zum Beispiel Standort oder Notizen
Remote	Einzelne Befehle an das Gerät senden („Befehl an Gerät senden“) mit Verlauf der Ergebnisse
Fernwartung & Konsole	Befehlszeile direkt im Browser

5.2 Patches installieren

The screenshot shows the Nexus RMM interface for device FS-SRV-01. The 'Patches' tab is active, displaying a list of 28 pending updates. The updates are listed in a table with columns: NAME, AKTUELL, VERFÜGBAR, and SCHWEREGRAD. Each update has an 'Installieren' button. The left sidebar shows the navigation menu with 'Geräte' selected. The top navigation bar shows various tabs like 'Übersicht', 'Sensoren', 'Tickets', etc., with 'Patches (28)' highlighted and a red circle with the number 1 next to it.

Reiter „Patches“ mit den ausstehenden Updates.

1 Reiter **Patches**. Die Zahl zeigt, wie viele Updates anstehen.

1. Öffne den Reiter **Patches**.
2. Klicke bei einem Update auf **Installieren**. Die Schaltfläche zeigt „Angestoßen...“, darunter „Wartet auf das Gerät“ oder „Läuft auf dem Gerät ...“ und zuletzt „Erledigt ✓“ oder „Fehlgeschlagen“.
3. Der Agent holt den Auftrag innerhalb weniger Sekunden ab. Du musst nicht auf den nächsten Check-in warten.

Hinweis

Bei Linux-Servern mit `apt` werden Updates zurückgehalten, die Ubuntu schrittweise ausrollt („phased updates“). Das RMM installiert sie trotzdem, wenn du sie ausdrücklich anstößt. Auf Linux braucht der Agent dafür root-Rechte oder `sudo` ohne Passwort. Der mitgelieferte Dienst läuft als root.

5.3 Konsole und Fernwartung

The screenshot shows the RMM interface for device FS-SRV-01. The sidebar on the left contains navigation links: Übersicht, Geräte (selected), Tickets, Angebote & Rechnungen, Kontakte, Software-Lizenzen, Serviceverträge, Passwörter, Dokumentation, Dateien, Webseiten, Alarme (3), Benutzer, and a DESIGN section with System (selected), admin (Admin), Passwort ändern, and Abmelden. The main content area has a top bar with links: Zurück, QR-Code / Etikett, Hardware-Doku (PDF), Agent-Installer (EXE), ZIP, and Bearbeiten. Below this is a 'Gerät löschen' button. The device status is 'Offline'. Other metrics include 'LETZTER CHECK-IN' (09.10.2026, 16:30), 'AGENT-VERSION' (1.0.0.48), 'UPTIME' (0 h), 'NEUSTART AUSSTEHEND' (Nein), 'PATCHES OFFEN' (28), 'VOLUMES < 10 % FREI' (2), 'VIRENSCHUTZ' (-), and 'FEHLER (24 H)' (0). A horizontal menu below these metrics includes: Übersicht, Sensoren, Tickets (0), Dokumentation (0), Datenträger (9), Netzwerk (3), Hardware (1), Software (500), Patches (28), Dienste (0), Prozesse, Sicherheit & Benutzer, Ereignisse (0), Felder, Remote, and 'Fernwartung & Konsole' (highlighted with a red box and a red circle 1). The 'Fernwartung & Konsole' section contains text about Live-Fernwartung, Bildschirmfreigabe (einfach), PowerShell, and Dateimanager. Below this text are four buttons: 'Live-Fernwartung starten' (2), 'Bildschirmfreigabe (einfach)' (3), 'PowerShell öffnen' (4), and 'Dateimanager öffnen' (5). A checkbox 'Vor dem Start nachfragen' (6) is checked.

Reiter „Fernwartung & Konsole“.

- 1 Reiter **Fernwartung & Konsole**.
- 2 **Live-Fernwartung starten**: flüssiges Remote-Desktop für Windows-Geräte (bis etwa 20 Bilder pro Sekunde, mehrere Monitore, Maus und Tastatur).
- 3 **Bildschirmfreigabe (einfach)**: der bisherige Weg mit 2 bis 8 Bildern pro Sekunde. Er braucht keinen Zusatzdienst und dient als Rückfall.
- 4 **PowerShell öffnen**: eine Konsole im Browser mit den Rechten des Agenten (normalerweise SYSTEM).
- 5 **Dateimanager öffnen**: Ordner durchsuchen, Dateien herunterladen und hochladen (Windows, Linux und NAS).
- 6 **Vor dem Start nachfragen**: mit Häkchen fragt der Browser vor der Bildschirmfreigabe nach. Ohne Häkchen startet sie sofort.

Bei **Linux-Geräten** öffnest du mit **SSH-Konsole öffnen** eine Shell, wie bei einer SSH-Sitzung, aber ohne SSH-Zugang. Bei **Windows-Geräten** nutzt du **Live-Fernwartung starten**, um den Bildschirm zu sehen und Maus und Tastatur zu steuern. Das Gerät verbindet sich dabei von innen nach außen mit deinem

Server. Es sind weder offene Ports noch ein VPN noch eine feste IP nötig. PowerShell und die SSH-Konsole dürfen nur Benutzer mit der Rolle „admin“ öffnen.

Live-Fernwartung einrichten (einmalig, auf dem Server)

Die Live-Fernwartung und der Dateimanager brauchen einen kleinen Dienst auf dem Server, den Relay. Er besteht nur aus Python und läuft lokal. Apache reicht ihn über dein HTTPS durch. Ohne den Relay bleibt der Knopf **Live-Fernwartung starten** grau, und der Dateimanager startet nicht. Die einfache Bildschirmfreigabe funktioniert weiter.

1. Spiele das RMM-Update ein. Der Ordner `relay` liegt danach im RMM-Verzeichnis.
2. Führe auf dem Server aus (Pfad deinem RMM-Ordner anpassen): `sudo bash /var/www/rmm/relay/install_relay.sh`.
3. Das Skript legt das gemeinsame Geheimnis `data/relay_secret` an, richtet den Dienst `h74-relay` ein, aktiviert die Apache-Module `proxy` und `proxy_wstunnel` und trägt die Weiterleitung `/relay/ws` in die `.htaccess` ein. Am Ende meldet es „OK: Relay läuft“.
4. Öffne bei einem Windows-Gerät **Fernwartung & Konsole**. Der Knopf **Live-Fernwartung starten** ist jetzt blau.

```
sudo bash /var/www/rmm/relay/install_relay.sh
systemctl status h74-relay
curl http://127.0.0.1:8765/health
```

Hinweis

Die Windows-Agenten holen den neuen Programmcode selbst (Overlay-Update). Es muss keine neue EXE gebaut werden. Der Agent braucht die Pakete `mss` und `Pillow`, die auch die einfache Bildschirmfreigabe nutzt.

Mit der Live-Fernwartung arbeiten

- Klicke **Live-Fernwartung starten**. Nach wenigen Sekunden erscheint der Bildschirm des Geräts. Auf dem Gerät erscheint keine Abfrage. Im Browser fragt das RMM vorher nach, solange **Vor dem Start nachfragen** angehakt ist. Nimm das Häkchen heraus, wenn die Sitzung sofort starten soll. Der Browser merkt sich die Einstellung.
- Die Live-Fernwartung zeigt auch den Anmeldebildschirm und den gesperrten Bildschirm. Du kannst dich also aus der Ferne als Administrator am Gerät anmelden.
- Klicke ins Bild, um Maus und Tastatur zu steuern. Mit dem Mausrad scrollst du, **Vollbild** vergrößert die Ansicht.
- Bei mehreren Monitoren wählst du über die Auswahl oben den Monitor oder **Alle Monitore**.
- Über die Tastenleiste über dem Bild sendest du **Strg+Alt+Entf**, die **Windows-Taste**, Win+R, Win+E, Win+D, Win+L, Alt+Tab und den Task-Manager. Im **Vollbild** (Chrome oder Edge) gibt der Browser die ganze Tastatur weiter, auch Windows-Taste und Alt+Tab. Der Mauszeiger des Geräts ist im Bild nicht sichtbar, du siehst deinen eigenen Zeiger.

- Mit **Verbindung beenden** schließt du die Sitzung. Sie endet sonst nach spätestens 4 Stunden oder sobald eine Seite die Verbindung verliert.

Dateimanager

Der Dateimanager zeigt die Ordner und Dateien eines Geräts im Browser, auch bei Linux-Geräten und NAS ohne SSH. Er nutzt denselben Relay wie die Live-Fernwartung (Einrichtung siehe oben) und läuft mit den Rechten des Agenten. Deshalb dürfen ihn nur Benutzer mit der Rolle „admin“ öffnen.

The screenshot shows the 'Dateimanager - aktiv' window for device 'FS-SRV-01'. The interface includes a sidebar with navigation options and a main area displaying the file manager. The file list shows the following files:

NAME	GRÖSSE	GEÄNDERT
Berichte		10.10.26, 14:36
Sicherungen		10.10.26, 14:36
Skripte		10.10.26, 14:36
Anleitung.txt	11 B	10.10.26, 14:36
Inventar-Export.csv	1.8 MB	10.10.26, 14:36
Netzwerkplan.pdf	512 KB	10.10.26, 14:36

Dateimanager mit Ordnern und Dateien eines Geräts.

- 1 Pfad:** zeigt den aktuellen Ordner. Tippe einen Pfad ein und drücke Enter, um direkt dorthin zu springen. Bei Windows beginnst du mit der Laufwerksliste, bei Linux mit `/`.
- 2 Hochladen:** wählt Dateien auf deinem Rechner aus und legt sie im aktuellen Ordner ab. Du kannst Dateien auch per Drag & Drop in das Fenster ziehen.
- 3 Herunterladen:** lädt die Datei auf deinen Rechner.
- 4 Löschen:** entfernt die Datei oder den Ordner nach einer Rückfrage. Neben dem Papierkorb liegen **Umbenennen** (Stift) und oben **Neuer Ordner**.

Hinweis

Beim Hochladen fragt der Dateimanager nach, bevor er eine vorhandene Datei überschreibt. Jede Aktion (Herunterladen, Hochladen, Löschen, Umbenennen, Ordner anlegen) steht im Audit-Log. Ein Ordner mit Inhalt wird erst nach einer zweiten Rückfrage gelöscht.

5.4 Sensoren und Alarme

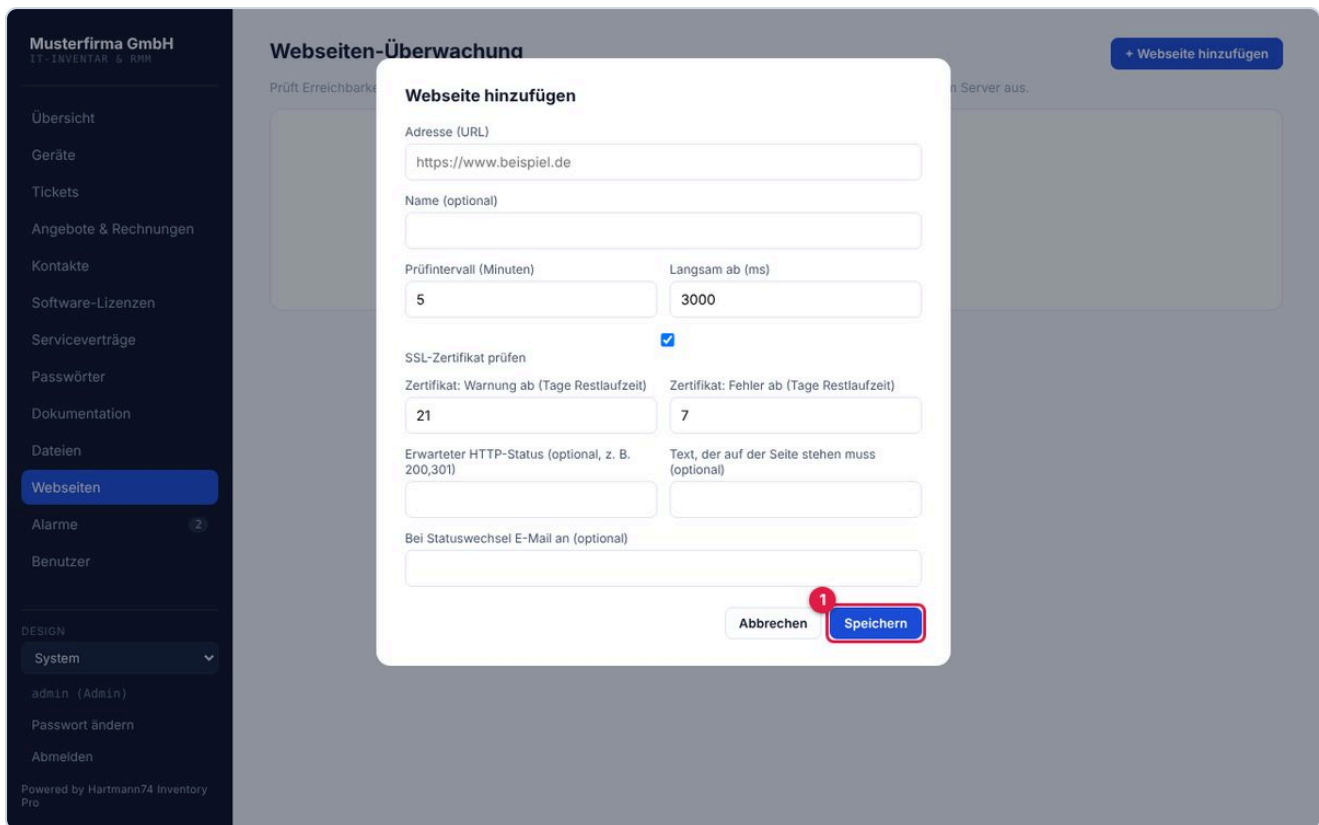
Reiter „Sensoren“ mit Auslastung und Schwellwerten.

1 Reiter **Sensoren**.

Der Agent überwacht Speicherplatz, Arbeitsspeicher, CPU und Netzwerk. Überschreitet ein Wert seinen Schwellwert, entsteht ein **Alarm**. Alle offenen Alarme siehst du im Menü **Alarme** (im Kundenbereich) und unter **Sensor-Alarme** (in der Plattform-Verwaltung, kundenübergreifend).

5.5 Webseiten überwachen

Im Menü **Webseiten** trägst du Adressen ein, zum Beispiel <https://www.kunde.de>. Geprüft werden Erreichbarkeit, Antwortzeit und das SSL-Zertifikat (Ablaufdatum, Name, Aussteller). Optional prüfst du einen erwarteten Status (zum Beispiel 200) oder einen Text auf der Seite und lässt dich bei Statuswechsel per E-Mail benachrichtigen.



Dialog „Webseite hinzufügen“.

- 1 Nach dem Ausfüllen auf die blaue Schaltfläche klicken.

Damit die Prüfungen automatisch laufen, richtest du einmalig einen Cron-Job ein (Abschnitt 6.2). Ohne Cron kannst du jederzeit auf **Jetzt prüfen** klicken. Interne Adressen wie `localhost` oder `192.168.x.x` sind aus Sicherheitsgründen gesperrt.

5.6 Tickets

Im Menü **Tickets** erfassen du und dein Kunde Störungen. Tickets lassen sich Geräten zuordnen, Kategorien und Zuweisungsregeln helfen bei der Verteilung, SLA-Zeiten steuern die Reaktionsfristen. Die Einstellungen dafür findest du in der Plattform-Verwaltung unter **Ticket-Verwaltung** (Reiter Kategorien, Tags, Zuweisungsregeln, SLA, Vorlagen, E-Mail, Checklisten).

5.7 Benutzer und Rollen

Im Kundenbereich legst du unter **Benutzer** weitere Mitarbeiter an. Es gibt zwei Rollen:

Rolle	Rechte
admin	Darf alles ansehen, ändern, löschen und Remote-Befehle ausführen
readonly	Darf alles ansehen (auch gespeicherte Passwörter), aber nichts anlegen, ändern oder löschen und keine Remote-Befehle ausführen

Weitere Bereiche des Kundenbereichs sind Angebote & Rechnungen, Kontakte, Software-Lizenzen, Serviceverträge, Passwörter (verschlüsselt gespeichert), Dokumentation und Dateien.

6 Server-Einstellungen

6.1 E-Mail über Microsoft 365 (Graph)

Das RMM kann Ticket-Antworten, Warnungen, Mahnungen und Meldungen der Webseiten-Überwachung über Microsoft 365 versenden und ein Support-Postfach auslesen. Dafür braucht es kein Passwort im RMM.

1. Öffne `portal.azure.com` → Microsoft Entra ID → App-Registrierungen → **Neue Registrierung** (Name zum Beispiel „RMM Mail“). Notiere „Anwendungs-ID (Client)“ und „Verzeichnis-ID (Mandant)“.
2. Öffne **API-Berechtigungen** → **Berechtigung hinzufügen** → **Microsoft Graph** → **Anwendungsberechtigungen**. Wähle `Mail.Send`, `Mail.Read` und `Mail.ReadWrite`. Klicke danach auf **Administratorzustimmung erteilen**.
3. Öffne **Zertifikate & Geheimnisse** → **Neuer geheimer Clientschlüssel**. Kopiere sofort den **Wert** (nicht die ID). Er wird nur einmal angezeigt.
4. Empfohlen: Beschränke die App per Exchange-Online-PowerShell (`New-ApplicationAccessPolicy`) auf das eine Support-Postfach, damit sie nicht alle Postfächer lesen darf.
5. Öffne im RMM **Plattform-Verwaltung** → **Ticket-Verwaltung** → **Reiter E-Mail**. Setze das Häkchen bei „E-Mail-Integration aktiviert“, wähle den Mail-Weg „Microsoft 365: Graph“ und trage Verzeichnis-ID, Anwendungs-ID, Clientschlüssel und das Postfach ein (zum Beispiel `support@deine-firma.de`).
6. Klicke auf **Speichern** und danach auf **Testmail senden**.

Hartmann74 Inventory Pro
PLATTFORM-VERWALTUNG

Suchen (Tickets, Kontakte, Wissensdatenbank, Dokumente)

Ticket-Verwaltung

Kategorien Tags Zuweisungsregeln SLA Vorlagen **E-Mail** Checklisten

Tickets per E-Mail

Eingehende E-Mails an das konfigurierte Postfach werden zu Tickets (neuer Absender) oder als Antwort einem bestehenden Ticket zugeordnet (per Bezugs-Kopfzeile oder „#123“ im Betreff). Mitarbeiter-Antworten können optional per E-Mail an den Kunden gesendet werden.
Hinweis: Die PHP-IMAP-Erweiterung ist auf diesem Server nicht installiert (php-imap) – der automatische Postfachabruf funktioniert erst danach.

☐ E-Mail-Integration aktiviert

Mail-Weg
 Klassisch: IMAP + SMTP

Posteingang (IMAP)

Server: imap.ionos.de Port: 993
 Ordner: INBOX ☒ SSL/TLS
 Benutzer: Passwort:

Postausgang (SMTP)

Server: smtp.ionos.de Port: 587
 Verschlüsselung: STARTTLS Benutzer:

Ticket-Verwaltung → Reiter „E-Mail“.

- 1 Reiter **E-Mail**. Dort stehen auch Posteingang und Postausgang für den klassischen Weg über IMAP und SMTP.

Hinweis

Der Clientschlüssel läuft nach spätestens 24 Monaten ab. Erzeuge dann einen neuen und trage ihn ein.

6.2 Automatische Aufgaben (Cron)

Zwei Skripte laufen regelmäßig. Öffne den Cron des Webserver-Benutzers mit `sudo crontab -u www-data -e` und füge ein:

```
* * * * * /usr/bin/php /var/www/rmm/cron/webseiten_check.php >> /var/log/h74-webseiten.log 2>&1
*/5 * * * * /usr/bin/php /var/www/rmm/cron/ticket_mail_poll.php >> /var/log/h74-mail.log 2>&1
```

Die erste Zeile prüft die überwachten Webseiten (jede nur in ihrem eigenen Intervall, Standard 5 Minuten). Die zweite ruft das Support-Postfach ab und erzeugt Tickets aus E-Mails. Alternativ rufst du das Postfach im Reiter E-Mail manuell mit **Postfach jetzt abrufen** ab.

6.3 Zwei-Faktor-Anmeldung

Aktiviere sie für alle Administratoren. Du findest sie in der Plattform-Verwaltung links unten unter **Sicherheit (2FA)** und im Kundenbereich unter dem eigenen Konto. Du brauchst eine Authenticator-App

(Microsoft Authenticator, Google Authenticator und ähnliche).

6.4 Weitere Einstellungen

In der Plattform-Verwaltung findest du **Einstellungen** (Branding mit Logo und Farben), **Audit-Log** (wer hat wann was geändert) und **Alle Geräte** (kundenübergreifende Liste). Mit **Design** links unten wählst du helles oder dunkles Erscheinungsbild.

7 Sicherung und Updates

7.1 Sichern

Sichere regelmäßig, am besten täglich per Cron, und lege die Sicherung außerhalb des Servers ab:

```
mysqldump -u nexusrmm -p nexusrmm > rmm-backup.sql  
tar czf rmm-data.tar.gz /var/www/rmm/data /var/www/rmm/config.php
```

Wichtig ist der Ordner `data/`. Er enthält `secret.key` und Anhänge. Ohne `secret.key` sind gespeicherte Passwörter unbrauchbar.

7.2 Server aktualisieren

The screenshot shows the 'System-Update' interface of the Hartmann74 Inventory Pro Platform Management. On the left is a dark sidebar with navigation links: Dashboard, Mandanten, Alle Geräte, Sensor-Alarme, Tickets, Ticket-Verwaltung, Leistungsplaner, Kalender & Aufgaben, Zeiterfassung & Personal, Angebote & Rechnungen, Warenwirtschaft, Reporting, Dokumentation, Kontakte, Dateien, Mitarbeiter, Einstellungen, and Lizenz. The main content area has a search bar at the top. Below it, the 'System-Update' section shows a message: 'Keine Lizenz hinterlegt (Lizenz-Seite). (geprüft 15:56:56) Erneut prüfen'. Below this, the 'Aktuelle Version: 1.0.0.49' is displayed. A detailed text block explains the update process: 'Hier kann ein Update-ZIP (wie du es im Chat erhältst) direkt eingespielt werden, statt Dateien manuell per FTP zu kopieren. Ablauf: zuerst eine Vorschau (ändert noch nichts), danach erst – nach Bestätigung – das echte Einspielen. Dabei wird automatisch ein Sicherungs-ZIP aller betroffenen Dateien angelegt, bevor etwas kopiert wird. Die Ordner data/ (Lizenz-Schlüssel, Verschlüsselung, Backups), config.php, agent_dist/ (individuell gebaute Windows-Agents) und .htaccess werden dabei NIE angefasst. Das ersetzt keine reguläre Datenbank-Sicherung vor größeren Updates – bei wichtigen Zwischenständen zusätzlich selbst ein DB-Backup ziehen.' Below this text is a section for 'Update-ZIP auswählen' with a 'Choose File' button and the text 'No file chosen'. At the bottom of this section is a blue button labeled 'Vorschau laden'. In the top right corner of the main area, there is a link: 'Update-Paket hochladen und einspielen'.

Plattform-Verwaltung → System-Update.

1 Die Seite „System-Update“.

1. Lade die neue Version aus deinem Kundenkonto auf hartmann74.com herunter.
2. Mache zuerst eine Sicherung der Datenbank (Abschnitt 7.1).
3. Öffne **Plattform-Verwaltung** → **System-Update**, lade das ZIP hoch, prüfe die Vorschau und bestätige.
4. Das Update sichert die überschriebenen Programmdateien. `config.php`, `data/` und `.htaccess` bleiben unverändert. Datenbank-Änderungen laufen automatisch.

Hinweis

Das Hochladen des Updates ist größer als das PHP-Standardlimit. Die mitgelieferte `.htaccess` erhöht es. Läuft PHP über FPM, setze in der `php.ini`: `upload_max_filesize = 100M` und `post_max_size = 120M`.

7.3 Agenten aktualisieren

Die Agenten aktualisieren sich selbst. Nach einem Server-Update erkennt jeder Agent beim nächsten Check-in die neue Version, lädt sie vom Server und startet neu. Das dauert etwa eine Minute pro Gerät. Die aktuelle Agent-Version steht pro Gerät auf der Detailseite. Du musst nichts neu installieren.

8 Fehlersuche

Problem	Lösung
Live-Fernwartung bleibt grau oder verbindet nicht	<code>systemctl status h74-relay</code> prüfen, dann <code>curl http://127.0.0.1:8765/health</code> (muss „ok“ melden). <code>a2query -m proxy_wstunnel</code> muss „enabled“ zeigen, im Virtual Host muss <code>AllowOverride All</code> gelten. Hinter einem zusätzlichen Proxy (zum Beispiel Cloudflare) muss WebSocket erlaubt sein
Seite zeigt 404 oder bleibt leer	<code>sudo a2enmod rewrite</code> , im Virtual Host <code>AllowOverride All</code> setzen, Apache neu laden
„Internal Server Error“ direkt nach dem Hochladen	<code>/var/log/apache2/error.log</code> prüfen. Meist fehlt das Apache-Modul <code>headers</code> , oder die <code>.htaccess</code> enthält <code>php_value</code> -Zeilen, die dein PHP-Betrieb nicht erlaubt (bei PHP-FPM löschen und Werte in <code>php.ini</code> setzen)
Installer meldet „Schreibrechte fehlen“	<code>sudo chown -R www-data:www-data /var/www/rmm</code>
Installer meldet „bereits eingerichtet“	Es gibt schon eine <code>config.php</code> . Nur bei bewusster Neu-Einrichtung löschen (zusammen mit <code>data/secret.key</code>), vorher alles sichern
Lizenz wird abgelehnt	Schlüssel komplett und ohne Leerzeichen einfügen. Bei weiteren Problemen schreibe an den Support (Adresse in der Bestellbestätigung)
Gerät bleibt offline	Auf dem Gerät <code>server_url</code> in <code>agent_config.json</code> prüfen (erreichbar, HTTPS-Zertifikat gültig). Windows: Aufgabe „Hartmann74 Agent“ läuft? Linux: <code>systemctl status h74-agent</code> . Synology: Ausgelöste Aufgabe ausführen und <code>agent.log</code> ansehen
Windows-Installer (EXE) fehlt im Dialog	<code>agent_dist/Hartmann74_Agent.exe</code> liegt nicht auf dem Server (Abschnitt 4.5). Das ZIP funktioniert trotzdem
Patches werden nicht installiert (Linux)	Agent muss als root laufen oder <code>sudo</code> ohne Passwort haben. Ergebnis steht in der Zeile des Patches
Webseiten-Prüfung läuft nicht	Cron-Eintrag aus Abschnitt 6.2 prüfen, Protokoll <code>/var/log/h74-webseiten.log</code> ansehen

9 Sicherheit

- Betreibe das RMM nur über HTTPS und lösche `install.php` nach der Einrichtung.
- Verwende starke, einzigartige Passwörter und aktiviere die Zwei-Faktor-Anmeldung für alle Administratoren.
- Handle Agent-Schlüssel wie Passwörter. Das ZIP nach der Installation löschen.
- Sichere `config.php` und `data/secret.key` getrennt vom Server.
- Halte Betriebssystem, PHP und MariaDB aktuell.

Support: <https://hartmann74.com>