ANWENDEN. VERSTEHEN. NACHVOLLZIEHEN.

Installation und Betrieb V2-Pilot

Uptime Control 2.0.0-alpha.1

Detaillierte Abläufe, klare Zuständigkeiten und nachvollziehbare Kontrollen.

Ausgabe 25. November 2026
Linux x86_64 + Docker | Dokumentation des V2-Pilotstands

Keine echten Kundendaten in Abbildungen. Nutzungsrechte richten sich nach der gesonderten Vereinbarung.

Inhalt

01 Geltungsbereich und Ihr Weg durch V2 3

02 Anmeldung, zweiter Faktor und Sitzungsende 4

03 Pilotinstallation vorbereiten 7

04 Konfigurieren und installieren 8

05 Lizenz online oder per QR-Code aktivieren 9

06 Betrieb, Sicherung und Wiederherstellung 10

07 Durchgängige Übung und Abnahme 11

01 Geltungsbereich und Ihr Weg durch V2

Diese Ausgabe beschreibt 2.0.0-alpha.1 anhand des lokalen Quellstands und der Pilotunterlagen vom 21./22.11.2026. Dokumentationsstand: 25.11.2026. Der Versionsname bezeichnet einen Pilotstand; das Handbuch ist keine Produktivfreigabe. Die bestehenden Grundfunktionen werden mit den neuen Arbeitsabläufen gemeinsam erklärt.

1. Melden Sie sich mit Ihrem persönlichen Konto und zweitem Faktor an. Prüfen Sie Name, Standort und zugeteilte Anlagen.

2. Techniker beginnen mit dem geführten Serviceeinsatz. Serviceleitung richtet Prüfwege ein und bearbeitet offene Fälle. Lagerverantwortliche arbeiten im Lagerbereich.

3. Üben Sie zunächst an einem ausdrücklich freigegebenen Teststandort. Die Bilder zeigen erfundene Schulungsdaten, keine Kundenanlage.

4. Kontrollieren Sie nach jeder Buchung die Bestätigung und das gespeicherte Ergebnis. Ein ausgefülltes Formular ist noch keine Speicherung.

Die bisherigen Rollenhandbücher sind in diese Ausgabe übernommen und um V2-Kapitel ergänzt. Ältere Bildschirmbilder bleiben als Grundfunktionsansichten erkennbar; V2-Bilder stammen aus dem Pilot vom 21./22.11.2026. Sie dokumentieren diesen Stand und keine heute neu durchgeführte Betriebsabnahme.

Sprache und Bildschirmbegriffe

Die Serviceerfassung besitzt Deutsch und Englisch. Lager- und Vorlageneditor enthalten im vorliegenden Stand deutsche Beschriftungen. Englische Anleitungen nennen deshalb zusätzlich die sichtbaren deutschen Bedienelemente. Freitext wird nicht automatisch übersetzt.

02 Anmeldung, zweiter Faktor und Sitzungsende

Vorbereiten

Benötigt werden die vom Betreiber mitgeteilte HTTPS-Adresse, ein persönliches Konto und bei entsprechender Aufforderung eine Authenticator-App. Beispiele in diesem Handbuch sind keine realen Anmeldeadressen. Eine Zertifikatswarnung nicht übergehen.

1. Öffnen Sie die Adresse. Die Weiterleitung zum Anmeldedienst ist Bestandteil des normalen Ablaufs.

2. Tragen Sie Benutzernamen und Passwort in die dafür vorgesehenen Felder ein. Bei Aufforderung ändern Sie das Startpasswort nach der angezeigten Richtlinie.

3. Bei der ersten Einrichtung des zweiten Faktors scannen Sie den angezeigten QR-Code mit Ihrer eigenen Authenticator-App. Bestätigen Sie den aktuellen Einmalcode. Speichern oder verschicken Sie keinen Screenshot dieses QR-Codes.

4. Bei späteren Anmeldungen geben Sie den aktuellen Code ein. Ein abgelehnter Code kann abgelaufen sein: automatische Uhrzeit am Telefon prüfen und einen neuen Code abwarten.

5. Kontrollieren Sie nach der Anmeldung Name und Zuständigkeitsbereich. Interne und externe Techniker können unmittelbar im Serviceassistenten landen.

6. Wählen Sie bei Bedarf die Oberflächensprache. Sie ändert nicht die Sprache bereits gespeicherter Beschreibungen.

7. Melden Sie sich nach der Arbeit ausdrücklich ab. Ein geschlossenes Browserfenster bestätigt nicht automatisch eine serverseitige Abmeldung.

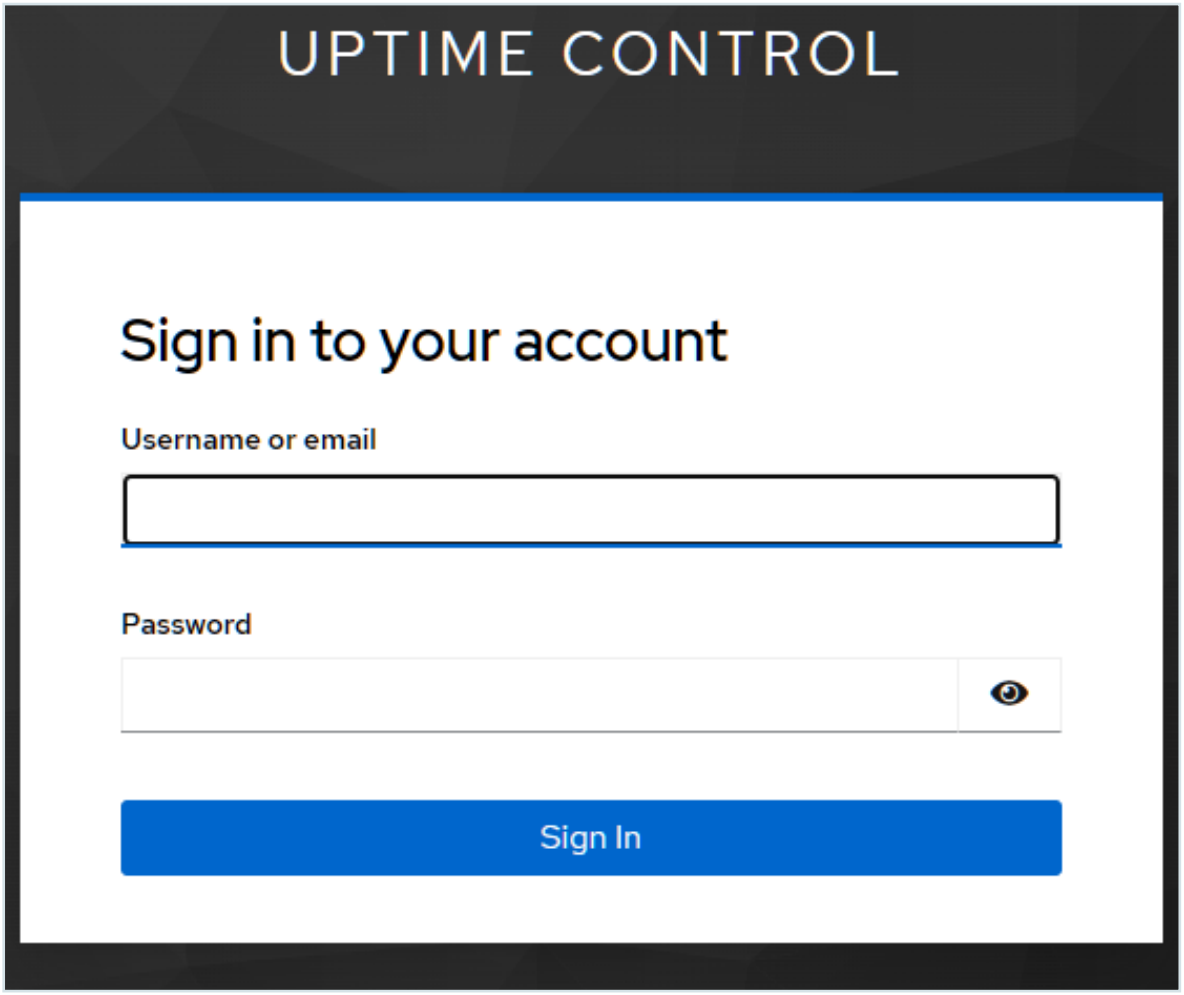
Telefon verloren oder gewechselt

Kontaktieren Sie einen bekannten Administrator. Nennen Sie die Kontokennung, niemals Passwort, Einmalcode oder Einrichtungsschlüssel. Nach identitätsgeprüfter MFA-Rücksetzung kann eine neue Anmeldung mit erneuter Einrichtung notwendig sein. Ein abgebrochener Rücksetzungsversuch darf nicht durch Löschen von Sicherheitsdatensätzen umgangen werden.

Sitzung während der Eingabe abgelaufen

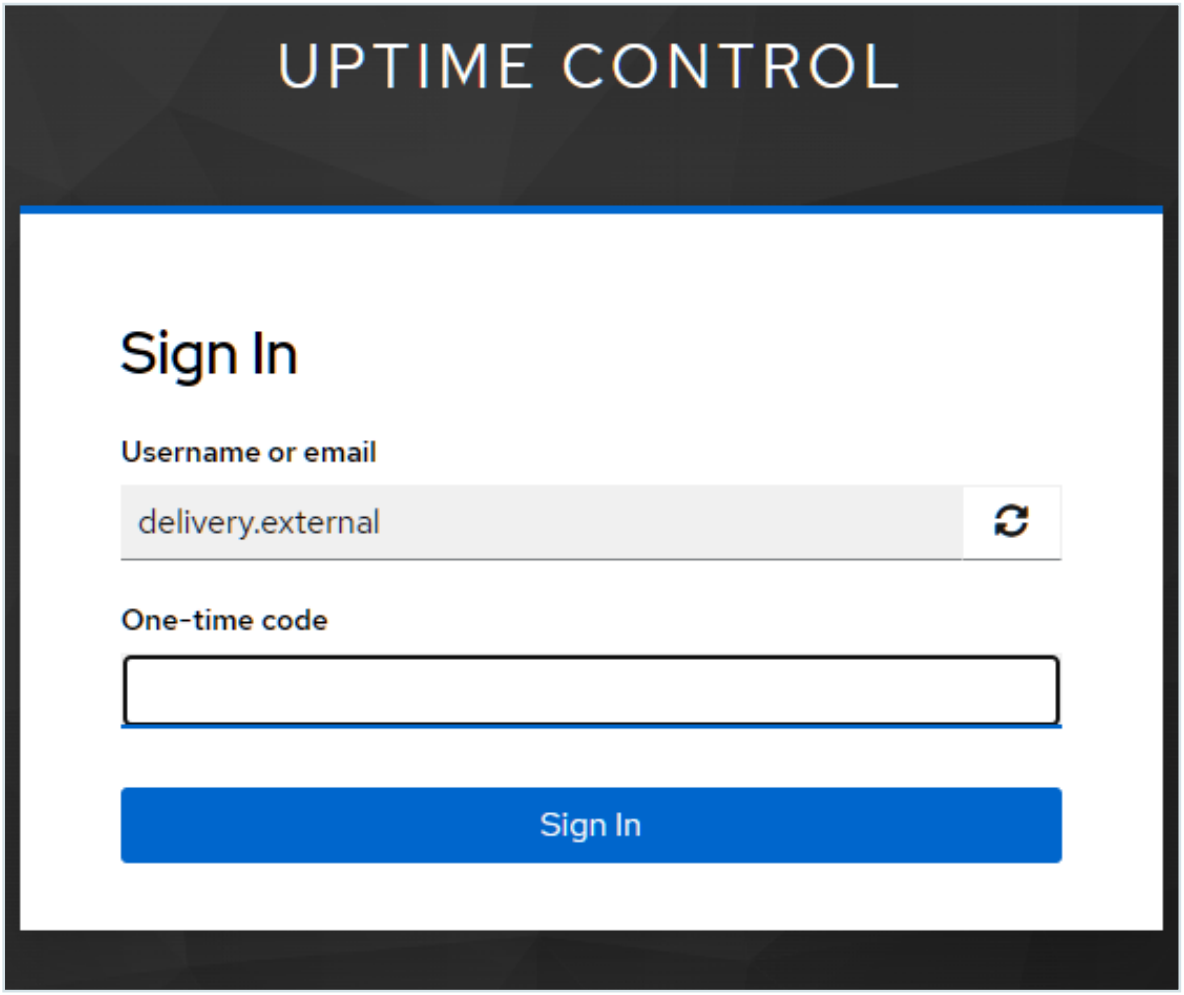
Erneut anmelden und zuerst prüfen, ob der zuletzt gesendete Vorgang gespeichert wurde. Erst danach erneut erfassen. Auf mobilen Geräten nach Netzwechsel ebenfalls die Speicherbestätigung kontrollieren.

Abbildung 1 | Persönliche Anmeldung. Die Sprache des Anmeldedienstes kann von der Anwendung abweichen.



Synthetische Schulungsdaten. V2-Aufnahmen: 21./22.11.2026; übrige Aufnahmen: Grundfunktionen der Vorgängerausgabe. Maßgeblich sind die Schritte im Kapitel.

Abbildung 2 | Zweiter Faktor: aktuellen Einmalcode verwenden; keine Einrichtungsgeheimnisse weitergeben.



Synthetische Schulungsdaten. V2-Aufnahmen: 21./22.11.2026; übrige Aufnahmen: Grundfunktionen der Vorgängerausgabe. Maßgeblich sind die Schritte im Kapitel.

03 Pilotinstallation vorbereiten

Diese Anleitung gilt für eine Neuinstallation des Pakets Uptime-2.0.0-alpha.1-Pilot.tar.gz. Sie ist keine Anleitung zum Überschreiben oder Migrieren einer V1-Installation. Verwenden Sie einen eigenen frischen Linux-Server oder eine eigene virtuelle Maschine.

Voraussetzungen

Linux x86_64 (amd64), lokaler Docker Engine mit Compose-Plug-in, Python ab 3.11, OpenSSL, tar und sudo. Planen Sie Speicher für Container, wachsende Datenbanken und getrennte Sicherungen ein. Konkrete Kapazitäten müssen zur erwarteten Nutzung passen.

Legen Sie zwei DNS-Namen fest: einen für die Anwendung und einen für den Anmeldedienst. Beide müssen aus dem Benutzernetz erreichbar sein. Standardports sind 443 und 8443. Prüfen Sie Portbelegung, Firewall und gegebenenfalls den vorgeschalteten Proxy.

Zertifikate

Das Zertifikat muss beide Namen abdecken und bei der Installation länger als sieben Tage gültig sein. Halten Sie Zertifikatskette und passenden privaten Schlüssel als Dateien auf dem Server bereit. Bei eigener Zertifizierungsstelle wird zusätzlich die vertrauenswürdige CA-Kette benötigt. Vermeiden Sie Zertifikatswarnungen durch korrekte Namensauflösung und Vertrauenskonfiguration.

Paket prüfen

Beziehen Sie das Installationspaket direkt von Medlix. Vergleichen Sie die mitgelieferte Prüfsumme vor dem Entpacken. Bei Abweichung nicht fortfahren.

```
sha256sum -c Uptime-2.0.0-alpha.1-Pilot.tar.gz.sha256

tar -xzf Uptime-2.0.0-alpha.1-Pilot.tar.gz

cd uptime-v2-pilot

sudo sh install.sh check

cp customer.example.json pilot.json
```

Führen Sie die Befehle im Verzeichnis aus, das Archiv und Prüfsummendatei enthält. Die Prüfung muss erfolgreich sein, bevor Sie konfigurieren.

04 Konfigurieren und installieren

Konfigurationsdatei bearbeiten

Öffnen Sie pilot.json in einem Texteditor. app_host und identity_host enthalten DNS-Namen ohne https://. app_port und identity_port enthalten freie TCP-Ports.

bind_address = 127.0.0.1 bindet an die lokale Schnittstelle für einen lokalen Proxy. 0.0.0.0 bindet an alle Schnittstellen; begrenzen Sie dann den Zugriff durch die Firewall auf das beabsichtigte Netz. Wählen Sie die Einstellung passend zur tatsächlichen Architektur.

admin_username, admin_name und admin_email beschreiben das erste Administratorkonto. certificate und private_key sind absolute Dateipfade. trust_ca verweist bei eigener CA auf deren PEM-Datei.

Einrichtung ausführen

```
sudo sh install.sh configure --config pilot.json
```

Geben Sie das neue Administratorkennwort zweimal ein. Die vorgesehene Länge beträgt 12 bis 128 Zeichen. Bewahren Sie Zugangsdaten nur im freigegebenen Passwortspeicher auf.

```
sudo sh install.sh install
```

```
sudo sh install.sh status
```

Standardziel ist /opt/uptime-control-v2-pilot. Bei einem abweichenden Ziel muss --directory bei allen nachfolgenden Befehlen denselben Pfad bezeichnen. Eine bestehende Installation wird nicht mit install aktualisiert.

Ergebniskontrolle

Prüfen Sie die Ausgabe und öffnen Sie die konfigurierte HTTPS-Adresse. ACTIVATION_REQUIRED vor der ersten Lizenzfreigabe ist ein erwarteter Zustand. Ein Containerstart allein bestätigt noch keine funktionierende Anmeldung.

Bei Fehlern zuerst DNS, Ports, Zertifikate und vollständige Befehlsausgabe prüfen. Keine Datenverzeichnisse löschen, um einen Installationsfehler zu übergehen. Geben Sie im Support nur bereinigte Meldungen ohne Kennwörter oder private Schlüssel weiter.

05 Lizenz online oder per QR-Code aktivieren

Onlineaktivierung

1. Öffnen Sie die konfigurierte HTTPS-Adresse der eigenen Installation.

2. Geben Sie den für diese Installation ausgestellten Kaufcode ein.

3. Wählen Sie „Online aktivieren“. Der Server benötigt dafür HTTPS-Zugang zu lizenz.medlix.de.

4. Warten Sie auf die Bestätigung und den Start der Fachanwendung.

5. Melden Sie sich mit dem eingerichteten persönlichen Konto an und richten Sie den zweiten Faktor ein.

Erstaktivierung im abgeschotteten Netz

1. Geben Sie den Kaufcode an der eigenen Uptime-Installation ein und wählen Sie „Mit QR-Code aktivieren“.

2. Scannen Sie den angezeigten QR-Code mit einem zweiten, internetfähigen Gerät. Der Uptime-Server selbst kann im internen Netz bleiben.

3. Prüfen Sie die HTTPS-Adresse lizenz.medlix.de und bestätigen Sie dort die Freischaltung.

4. Übertragen Sie den vollständig angezeigten, gruppierten Freischaltcode in das Feld „Freischaltcode“ am ursprünglichen Uptime-Bildschirm.

5. Wählen Sie „Freischaltung bestätigen“ und warten Sie auf den Start. Danach anmelden und MFA einrichten.

Der QR-Code enthält vertrauliche Aktivierungsangaben. Teilen Sie ihn nicht als Screenshot. Eine Aktivierung auf einem zweiten Gerät ersetzt nicht die Übernahme des Codes in der ursprünglichen Installation.

Gültigkeit und Fehler

Die Freigabe gehört zur Serverinstallation, nicht zu einem einzelnen Benutzer. Konten und Rollen werden anschließend separat verwaltet. Bei „bereits belegt“ oder ungültigem Code prüfen Sie die Zuordnung und stimmen einen Serverwechsel mit Medlix ab. Nicht mit wechselnden Codes oder einer neuen Identität experimentieren.

Prüfstand

Onlineaktivierung und Wiederanlauf bei unerreichbarem Lizenzdienst wurden am 22.11.2026 am Pilotpaket geprüft. Die QR-Erstaktivierung wurde in diesem V2-Paketlauf nicht erneut geprüft; dieser Ablauf ist aus der gemeinsamen Aktivierungsanleitung übernommen und gehört zur Abnahme, wenn er eingesetzt wird.

06 Betrieb, Sicherung und Wiederherstellung

Regelbetrieb

Prüfen Sie Erreichbarkeit von Anwendung und Anmeldung, Zertifikatslaufzeiten, verfügbaren Speicher und den Erfolg der Sicherungen. Benennen Sie Verantwortliche und Vertretung. Eine Sicherungsdatei allein beweist noch keine Wiederherstellbarkeit.

```
sudo sh install.sh status
```

```
sudo sh install.sh backup --backup-dir /srv/uptime-pilot-backups
```

Der Sicherungslauf kann Dienste vorübergehend anhalten. Planen Sie das Zeitfenster und kontrollieren Sie anschließend den Betriebszustand. Speichern Sie Sicherungen zugriffsgeschützt und zusätzlich getrennt vom laufenden Server. Sie enthalten vertrauliche Betriebs- und Identitätsdaten.

Geplanter Stopp und Start

```
sudo sh install.sh stop
```

```
sudo sh install.sh start
```

stop hält den konfigurierten Stack an und erhält die Daten. Prüfen Sie nach start Anmeldung, einen bekannten Datensatz und den Lizenzzustand. Ein absichtlich nicht erreichbarer Lizenzdienst darf nicht mit einem allgemeinen Netzwerkausfall verwechselt werden.

Wiederherstellung auf einem frischen Ziel

Verwenden Sie ein isoliertes, frisches Ziel und die passende Version des Installationswerkzeugs. Prüfen Sie Sicherungsarchiv, Berechtigungen, DNS und Zertifikate. Der Befehl restore-new ist für ein neues Ziel gedacht, nicht zum Überschreiben eines laufenden Produktivsystems.

```
sudo sh install.sh restore-new --archive /sicherer/pfad/sicherung.tar.gz
```

Ersetzen Sie den Beispielpfad durch das tatsächlich geprüfte Archiv. Ein abweichendes Zielverzeichnis wird mit --directory angegeben. Dokumentieren Sie vor dem Start Quelle, Ziel und verantwortliche Person. Verhindern Sie, dass Test und Original gleichzeitig dieselben externen Aufgaben übernehmen.

Erfolgskontrolle

Prüfen Sie Anmeldung, Rollen, bekannte Serviceereignisse, Berichtsarchive, Lagerbestände, Inventurhistorie und Lizenzidentität. Vergleichen Sie Stichproben mit dem gesicherten Ausgangsstand. Geben Sie das Ziel erst danach betrieblich frei.

Die Lizenzidentität und persistente Schlüssel müssen erhalten bleiben. Bei Ersatzhardware, unklarer Lizenzbindung oder fehlenden Schlüsseln zuerst Medlix kontaktieren. Ein Neuaufsetzen ist kein Ersatz für die Wiederherstellung.

07 Durchgängige Übung und Abnahme

Verwenden Sie einen freigegebenen Teststandort mit synthetischen Daten. Führen Sie die Übung nicht versehentlich in produktiven Beständen aus.

1. Administrator: Standort, Anlagen, Benutzer und passende Rollen prüfen. Ein Benutzer ohne Standortrecht darf die Daten nicht bearbeiten.

2. Lager: Einen Testartikel anlegen, fünf Stück als Wareneingang buchen und ein Etikett drucken. Bestand und Journal kontrollieren.

3. Technik: Einen Servicevorgang für eine bereits stillstehende Anlage erfassen. Beginn der Störung und eigene Arbeitszeit getrennt dokumentieren.

4. Prüfweg: Einen bekannten Fehlercode verwenden, Fragen beantworten und einen tatsächlich verwendeten Testartikel zuordnen.

5. Abschluss: Funktionstest dokumentieren, Wiederherstellungszeit erfassen und Bericht speichern. Lagerbestand muss zur tatsächlichen Entnahme passen.

6. Serviceleitung: Vorgang, Stillstand, Arbeitszeit und mögliche offene Prüfung nachvollziehen. Einen Folgefall mit Wiedervorlage separat testen.

7. Lager: Eine bezogene Rückgabe und eine Teillieferung testen. Bestand und offene Bestellmenge kontrollieren.

8. Inventur: Lagerplatz sperren, alle Artikel zählen, eine bewusst erzeugte Differenz prüfen, abschließen und CSV exportieren.

9. Gegenprobe: Eine zweite Inventur abbrechen. Keine Differenzbuchung darf daraus entstehen; der Platz muss wieder frei sein.

10. Betrieb: Abmeldung, erneute Anmeldung, MFA und die vereinbarte Sicherung prüfen. Ergebnisse mit Datum, Rolle, erwartetem und tatsächlichem Ergebnis dokumentieren.

Abnahmegrenze

Diese Übung ist eine Vorlage. Sie ist kein bereits unterschriebenes Kundenabnahmeprotokoll. Erfasst werden müssen zusätzlich die konkrete Installation, echte Geräte, Drucker, Kameras, Rechteverteilung und betriebliche Freigaben.