OPERATE. UNDERSTAND. VERIFY.

Installation and Operations V2 Pilot

Uptime Control 2.0.0-alpha.1

Detailed procedures, clear responsibilities and traceable checks.

Edition 25 November 2026
Linux x86_64 + Docker | V2 pilot documentation

No real customer data in illustrations. Usage rights follow the separate agreement.

Contents

01 Scope and your route through V2 3

02 Account, MFA and session: practical walkthrough 4

03 Prepare the pilot installation 8

04 Configure and install 9

05 Activate the licence online or by QR code 10

06 Operations, backup and restore 11

07 End-to-end exercise and acceptance 12

01 Scope and your route through V2

This edition describes 2.0.0-alpha.1 using local source code and pilot evidence dated 21/22 November 2026. Documentation date: 25 November 2026. This is a pilot build; a manual does not constitute production acceptance. Existing core functions and the new workflows are explained together.

1. Sign in with your personal account and second factor. Check your identity, site and assigned machines.

2. Technicians start with the guided intervention. Service managers configure procedures and handle open cases. Warehouse staff use the inventory workspace.

3. Practise only on an explicitly approved training site. Illustrations contain synthetic training data, not a customer installation.

4. After each posting, check the confirmation and the stored result. Completing a form is not the same as saving it.

The previous role guides are included and extended with V2 chapters. Older screenshots illustrate core functions; V2 screenshots were captured during the pilot on 21/22 November 2026. They document that build, not a new operational acceptance performed today.

Language and screen labels

The service workflow supports German and English. The warehouse and procedure editor retain German labels in this build. English instructions therefore also give the actual German control names. Free text is not automatically translated.

02 Account, MFA and session: practical walkthrough

Before signing in

Use the address supplied by your administrator and check the hostname. Do not bypass certificate warnings on a real installation. The synthetic addresses in screenshots are not customer login addresses.

1. Open the application in your supported browser. Follow its sign-in redirect to the organisation's identity service.

2. Enter your personal username and password. Do not use a colleague's account, even for an urgent repair.

3. If prompted to change an initial password, choose a unique password that satisfies the displayed policy. Store it through your approved password-management process.

4. If authenticator enrolment is required, use your approved authenticator, scan the displayed enrolment code and enter its current one-time code. Treat the enrolment secret as a credential; never include it in a service report or support screenshot.

5. At later sign-ins, enter the current code. If rejected, check the device clock and wait for a fresh code before retrying. Repeated guesses can make access recovery harder.

6. Confirm the identity shown in the application. Check the machine or airport scope before entering any data.

7. Select English where necessary. Internal and external technicians may land directly in the five-step service workspace rather than the analysis dashboard.

8. When finished, use Sign out. On shared devices, wait for confirmation and close the browser session. An unconfirmed sign-out message means that you must retry; closing a tab alone is not proof of server-side sign-out.

Lost authenticator or changed phone

Contact the administrator through a known route. Supply your account identifier, not your password or a live one-time code. The administrator must verify your identity before resetting MFA. A reset can end existing sessions and require new enrolment. Do not ask a colleague to submit work under their name while you recover access.

Expired session during work

If the application says the session expired or access was revoked, sign in again. Check whether a previous save received confirmation before recreating it. A locally retained form is not a guarantee that the server stored it. Verify the final record reference and state.

Success check

You can identify your signed-in account, permitted scope and intended task. If the expected machine is absent, request a scope correction; do not choose a similarly named machine to proceed.

Additional navigation and account notes

This manual covers the V2 pilot; established account workflows are retained from the preceding edition. Linux with Docker is the server platform; users work in a browser. The service and ticket module is enabled in the documented edition; individual role and scope permissions still apply.

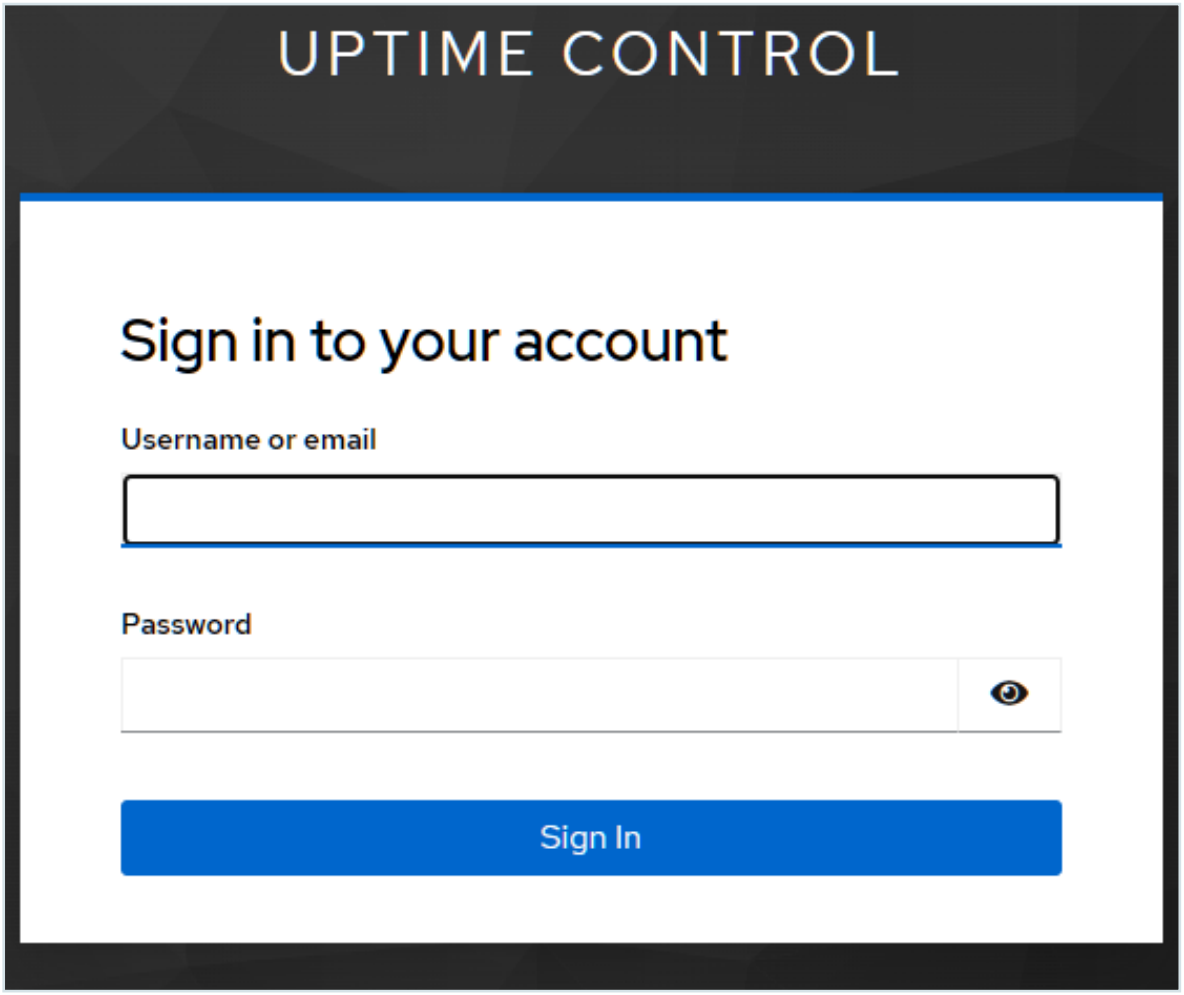
Open only the operator-provided HTTPS address. Use your personal account. The first administrator login in this installation package requires one-time-code enrolment. Scan the QR code only with your own authenticator app, confirm the current code, then sign in again. Do not retain or send pictures of the QR secret.

If a code is rejected, verify automatic phone time, wait for the next code and retry. Contact the designated administrator if the factor is lost. Browser and server clocks may differ; business day boundaries use the airport timezone.

After login, check your name, role and airport/machine scope. An account without an appropriate assignment has no business access. An empty screen after a new installation may be correct: no sample airports or customer records are created automatically.

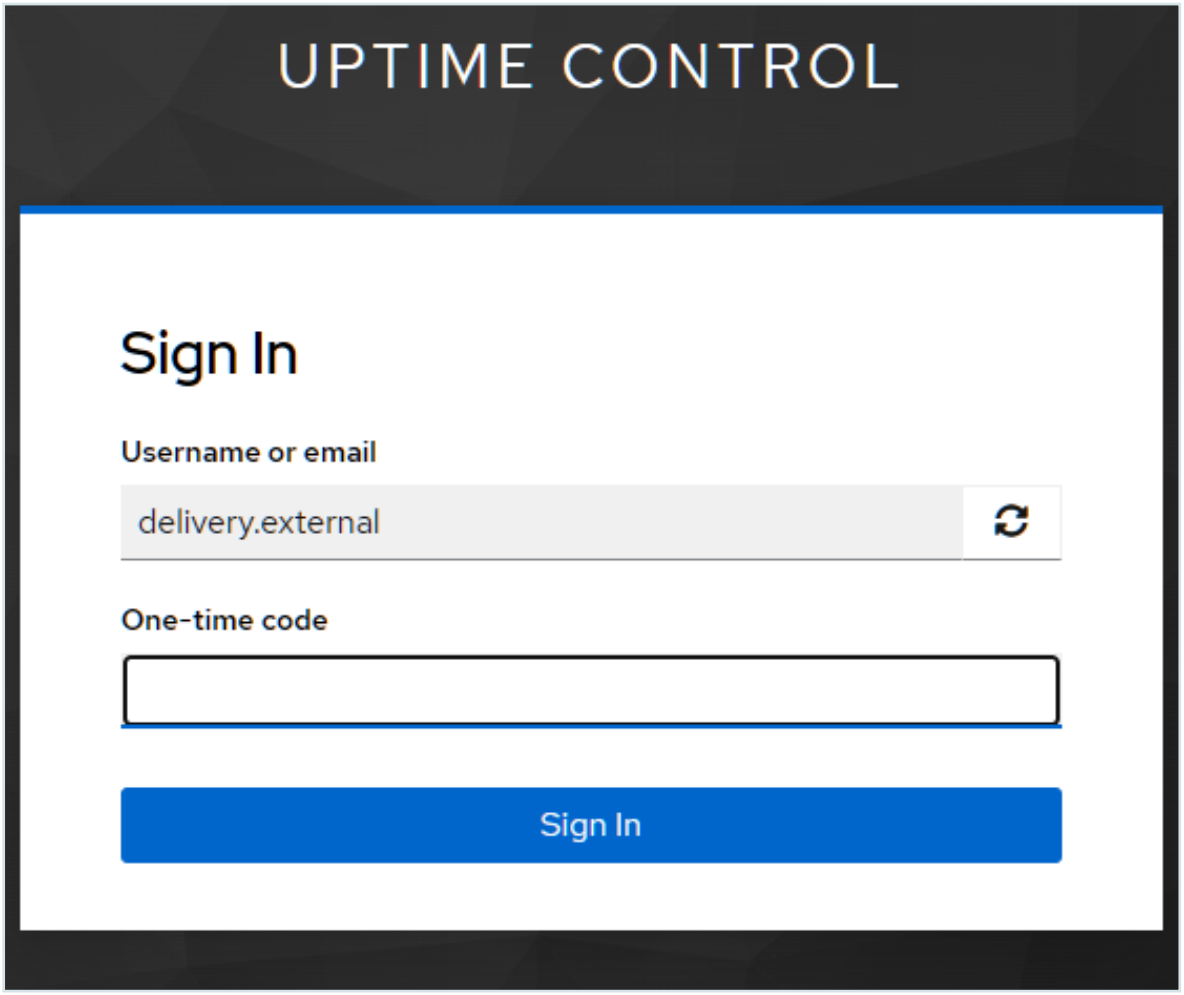
Before saving, check object, period, timezone, content and change reason. Wait for an unambiguous response. After a connection interruption, inspect the list or archive before creating another record. Sign out when finished, especially on shared devices.

Figure 1 | Personal sign-in: use the address and account supplied by your administrator.



Synthetic training data. V2 captures: 21/22 November 2026; other images: previous-edition core workflows. Some V2 screens retain German labels; the chapter explains their English meaning.

Figure 2 | MFA challenge: enter the current code from your own authenticator; never share it.



Synthetic training data. V2 captures: 21/22 November 2026; other images: previous-edition core workflows. Some V2 screens retain German labels; the chapter explains their English meaning.

03 Prepare the pilot installation

This procedure applies to a fresh installation of Uptime-2.0.0-alpha.1-Pilot.tar.gz. It does not overwrite or migrate a V1 installation. Use a separate fresh Linux server or virtual machine.

Requirements

Linux x86_64 (amd64), local Docker Engine with Compose plug-in, Python 3.11 or later, OpenSSL, tar and sudo. Allow storage for containers, growing databases and separate backups. Actual capacity must fit expected usage.

Choose two DNS names: one for the application and one for identity/sign-in. Both must be reachable from the user network. Default ports are 443 and 8443. Check port availability, firewall and any front-end proxy.

Certificates

The certificate must cover both names and remain valid for more than seven days at installation. Provide certificate chain and matching private key as server files. A private certificate authority also requires its trusted CA chain. Resolve name and trust configuration instead of bypassing certificate warnings.

Verify the package

Obtain the installer directly from Medlix. Compare the supplied checksum before extraction. Stop on any mismatch.

```
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
```

Run the initial commands in the directory containing the archive and checksum file. The check must succeed before configuration.

04 Configure and install

Edit configuration

Open pilot.json in a text editor. app_host and identity_host contain DNS names without https://. app_port and identity_port specify available TCP ports.

bind_address = 127.0.0.1 binds locally for a local proxy. 0.0.0.0 binds to all interfaces; restrict access to the intended network using the firewall. Choose according to the actual architecture.

admin_username, admin_name and admin_email describe the initial administrator. certificate and private_key are absolute file paths. trust_ca points to the private CA PEM file where applicable.

Run setup

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

Enter the new administrator password twice. The supported length is 12 to 128 characters. Store credentials only in the approved password manager.

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

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

The default target is /opt/uptime-control-v2-pilot. For a different target, --directory must refer to the same path in every subsequent command. install is not an updater for an existing installation.

Verify the result

Review command output and open the configured HTTPS address. ACTIVATION_REQUIRED before first activation is expected. A running container alone does not confirm working sign-in.

For failures, first check DNS, ports, certificates and full command output. Do not delete data directories to bypass installation errors. Share only sanitised support messages without passwords or private keys.

05 Activate the licence online or by QR code

Online activation

1. Open the configured HTTPS address of your own installation.

2. Enter the purchase code issued for this installation.

3. Choose online activation. The server needs HTTPS access to lizenz.medlix.de.

4. Wait for confirmation and application startup.

5. Sign in with the configured personal account and set up the second factor.

First activation in an isolated network

1. Enter the purchase code at your Uptime installation and select activation by QR code.

2. Scan the displayed QR code with a second device that has internet access. The Uptime server can remain on the internal network.

3. Verify the HTTPS address lizenz.medlix.de and confirm activation there.

4. Transfer the complete grouped activation code into the activation-code field on the original Uptime screen.

5. Confirm activation and wait for startup. Then sign in and configure MFA.

The QR code contains confidential activation information. Do not share it as a screenshot. Activation on the second device does not replace importing the code into the original installation.

Scope and errors

Activation belongs to the server installation, not an individual user. Accounts and roles are administered separately afterwards. For an already-assigned or invalid code, check its assignment and coordinate any server replacement with Medlix. Do not experiment with changing codes or a new identity.

Verification status

Online activation and restart with the licence service unavailable were checked against the pilot package on 22 November 2026. QR first activation was not repeated in that V2 package run; this procedure comes from the shared activation guide and must be included in acceptance if used.

06 Operations, backup and restore

Routine operations

Monitor application and sign-in availability, certificate expiry, free storage and backup success. Assign an owner and deputy. A backup file alone does not prove recoverability.

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

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

Backup can temporarily stop services. Schedule the window and check operational status afterwards. Restrict access and keep an additional copy separate from the running server. Backups contain confidential operational and identity data.

Planned stop and start

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

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

stop halts the configured stack while retaining data. After start, check sign-in, a known record and licence state. Do not confuse a deliberately unavailable licence service with a general network failure.

Restore to a fresh target

Use an isolated fresh target and the matching installer version. Verify backup archive, permissions, DNS and certificates. restore-new is intended for a new target, not overwriting a running production system.

```
sudo sh install.sh restore-new --archive /secure/path/backup.tar.gz
```

Replace the example path with the verified archive. Specify a different target directory with --directory. Record source, destination and responsible person before starting. Prevent test and original systems from performing the same external tasks simultaneously.

Verify success

Check sign-in, roles, known service records, report archives, stock balances, stocktake history and licence identity. Compare samples against the backed-up source. Release the target for operational use only afterwards.

Preserve licence identity and persistent keys. For replacement hardware, uncertain binding or missing keys, contact Medlix first. Reinstallation is not a substitute for restoration.

07 End-to-end exercise and acceptance

Use an approved test site with synthetic data. Do not accidentally perform this exercise against production stock.

1. Administrator: verify site, machines, users and roles. A user without site permission must not edit the data.

2. Warehouse: create a test article, receive five items and print a label. Check stock and journal.

3. Technician: record a service event for an already stopped machine. Keep outage onset separate from your own working time.

4. Guided path: use a known fault code, answer the questions and assign a test part actually used.

5. Completion: document the functional test, record restoration time and save. Stock must match the physical issue.

6. Service lead: trace event, downtime, working time and any outstanding review. Separately test a follow-up case with a review deadline.

7. Warehouse: test a referenced return and partial delivery. Check stock and outstanding order quantity.

8. Stocktake: lock the location, count all articles, investigate a deliberately introduced difference, complete and export CSV.

9. Counter-check: cancel a second stocktake. It must not post a difference and the location must become available again.

10. Operations: check sign-out, sign-in, MFA and the agreed backup. Record date, role, expected and actual outcome.

Acceptance boundary

This exercise is a template, not an already signed customer acceptance record. The actual installation, physical devices, printers, cameras, permission assignments and operational approvals must also be checked.