

Private server install guide

Install, run and connect your own Ubikron server.

November 2026 · ubikron.com/servers/install

Contents

1 **Introduction**
What the server is and where it runs

2 **Before you install**
Hardware, DNS and certificates, the install directory, security, Mac

3 **Local install**
The server on the same machine as your Chrome

4 **Dedicated server**
A separate machine that several investigators share

5 **Roll your own**
Your own DNS name and certificates

6 **Administration**
First sign-in, license, users, messages, updates, metrics

7 **Connecting the extension**
Signing your investigators in to your server

8 **Troubleshooting**
Forgotten password, Mac errors, slow starts, removing data

1. Introduction

You don't need to be a DevOps expert to install a Ubikron server, but you shouldn't be put off by a terminal.

The Ubikron private server is a stack of 11 Docker containers, with Mimic, our enrichment engine, included. One installer sets it all up. It runs:

1. on the same machine as your Chrome (localhost), on Windows, Mac or Linux;
2. on a machine in your own network, on your premises;
3. in a VPC, such as an EC2 or Linode instance.

Your investigators use the same Ubikron extension as everyone else. They just sign in to your server instead of ours.

The installer is called `ubikron-pro-server` on every platform. Download it from ubikron.com/servers/install: Windows, macOS (binary or PKG), Linux and Linux ARM64.

2. Before you install

Hardware

Ubikron loves memory. It runs with 16 GB available to Docker, but it really wants 32 GB. Cores matter less. A fast, stable connection between your investigators and the server makes a big difference too. The installer checks the machine before it starts:

	Minimum	Recommended
Processor	4 cores	8 cores
Memory available to Docker	16 GB	32 GB
Free disk space	20 GB	100 GB

You also need Docker installed and running. On Windows and Mac, Docker Desktop works well.

DNS and certificates

> **Installing on your own machine?** Skip this part. Everything stays inside your computer, so you don't need DNS or certificates.

- The extension and the server must talk over a real TLS connection. Self-signed certificates won't work. That's Chrome's rule, not ours.
- To make that easy, the installer creates a name and certificate for you under DNS4SSL.net, and renews the certificate. You only choose a name.
- A dash, two letters and two digits are added to the name you choose, so `test` becomes something like `test-pb56.dns4ssl.net`. That stops people guessing obvious names.
- Reinstalling and want the same name? Enter the full name, for example `test-pb56`, and you'll get it back, as long as you can reach the original IP address.
- You can use your own DNS name and certificates instead. See Roll your own.

The install directory

This is where the server lives and keeps all its data.

- Deleting the Docker containers, images and volumes doesn't touch it. **To remove all Ubikron data, delete this directory.**
- To reinstall without losing anything, point the installer at the same directory.

Security

We assume the server runs on your own computer or on a machine dedicated to Ubikron. We don't protect the server from other users on the same machine: access to the machine is access to Ubikron.

Securing the machine is up to you: strong passwords, closed unused ports, a firewall, no unneeded services. The server needs these ports open to your investigators:

Port	Purpose
80	HTTP, for certificate validation
443	HTTPS, the admin interface and API
7001	Communication with the Ubikron extension

Installing on a Mac

The Mac and Windows installers are signed. On a Mac, running the binary from the terminal makes macOS check that signature with Apple, which needs an internet connection. On a weak or missing connection the check fails with "Operation not permitted".

Use the **PKG installer** instead. It's stapled, so it verifies without contacting Apple, and it puts `ubikron-pro-server` in `/usr/local/bin`, ready to run from the terminal.

3. Local install

The server on the same machine as your Chrome extension. The usual way to try it without a VPC or a server of your own.

1. Make sure **Docker is installed and running**.
2. **Download** the installer for your operating system.
3. **Run the installer.** On a desktop it opens in your browser. To stay in the terminal, add `--cli`.
   - Linux and Mac: make it executable first with `chmod +x ubikron-pro-server`.
   - Linux: run it as root, for example `sudo ./ubikron-pro-server`.
4. Choose where to install, for example `d:\data\ubikron-server\` or `/data/ubikron-server`. The directories are created for you.
5. At "Select your install type", pick **Single user - install on Localhost only**.
6. Enter your **organisation identifier**: lowercase letters, digits and dashes, for example `acme-corp`.
7. Choose the **admin password**, at least 8 characters. It signs you in to both the Ubikron admin and Mimic.

Then the installer:

- generates random passwords for all the services;
- fetches the Docker images (be patient);
- starts the containers and waits for the server to come up. **The first start takes a while.**

When it says **Server is up!**, open the admin interface at the address it shows. See Administration.

```
# Linux / Mac: make it executable
$ chmod +x ubikron-pro-server

# Linux: run as root
$ sudo ./ubikron-pro-server

# Stay in the terminal instead of the browser
$ ./ubikron-pro-server --cli

# Use the browser installer even if no desktop is detected
$ ./ubikron-pro-server --gui
```

4. Dedicated server

The server on a separate machine: on your premises, in a private network, on a VM, or in a VPC. The normal setup when several investigators share a server.

1. Make sure **Docker is installed and running** on the server.
2. **Download** the installer for the server's operating system.
3. **Run the installer** (on Linux, as root with `sudo`). On a machine without a desktop it runs in the terminal.
4. Choose where to install, for example `/data/ubikron-server`.
5. At "Select your install type", pick **Multi-user - VPC / private network**.
6. **Choose a name** for your server, anything you'll remember. You get a DNS4SSL.net address for it, for example `test-pb56.dns4ssl.net`. That's the address you give your investigators.
   - If the name is taken, you're asked whether you want to reuse that name and IP address. Useful when reinstalling.
7. If the machine has more than one network interface, **select the one the name should point to**. All addresses are shown, the public one included, which helps if you forward ports. Pick the address your investigators' machines can reach.
8. Enter your **organisation identifier** and choose the **admin password** (at least 8 characters, for the admin and Mimic).

The installer then creates the name, gets the certificate, generates passwords, fetches the images and starts the server. A complete run looks like this:

```
$ sudo ./ubikron-pro-server --cli
Docker is already installed - good!
Docker is running - good!
Install in current directory? (y/n): n
Enter absolute path to install directory: /data/ubikron-server
System requirements:
OK Processor cores: 12 cores (minimum 4 cores, recommended 8 cores)
OK Memory available to Docker: 32 GB (minimum 16 GB, recommended 32 GB)
OK Free disk space: 180 GB (minimum 20 GB, recommended 100 GB)
Select your install type:
  1) Single user - install on Localhost only
  2) Multi-user - VPC /private network
Select option [1/2]: 2
Enter the DNS name you want to use (e.g. 'myserver' for myserver.dns4ssl.net): test
Generated DNS name: test-pb56.dns4ssl.net
Multiple IP addresses found:
  1) 203.0.113.23 (public)
  2) 10.0.0.170 (local)
  3) 192.168.56.1 (local)
Select interface / IP address to be used for DNS: 2
Requesting certificate from provider...
Certificate and key installed in /data/ubikron-server/certs
Generated passwords:
ELASTIC_PASSWORD: 4c1e9a07b2d5463f
POSTGRES_PASSWORD: 9b3f2e61c08a47d5
STORAGE_ACCESS_KEY: 51d0c7a39e6b48f2a1c4
```

```
STORAGE_SECRET_KEY: 0e7f3b9a2c5d4e81f6a7b0c3d9e2f5a8b1c4d7e0
JWT_BASE64_SECRET: q7Zr1V...(Base64, 512 bits)
Enter your organisation identifier (lowercase letters, digits and dashes, e.g. acme-corp): acme-corp
Choose a password for the admin account (used for both Ubikron and Mimic):
Repeat the admin password:
Admin password set. Sign in to Ubikron and Mimic as "admin" with this password.
[+] Pulling ...
✔ ubikron-seaweedfs  ✔ ubikron-elasticsearch  ✔ mimic  ✔ ubikron-wud
✔ ubikron-postgresql  ✔ ubikron  ✔ ubikron-logstash  ✔ zitadel
✔ ubikron-js-tools  ✔ ubikron-webserver  ✔ rabbitmq
[+] Running ...
Waiting for server to become available at: https://test-pb56.dns4ssl.net
Server is up!
You can access the server's admin interface at https://test-pb56.dns4ssl.net
Mimic is at https://test-pb56.dns4ssl.net/mimic/
A good first step is to create a user. Follow the online docs at https://ubikron.com/help/
Press Enter to close the installer.
```

The installation is complete. Go to Administration.

5. Roll your own: DNS and certificates

For organisations with their own PKI and full control of their DNS.

> Ubikron needs a real TLS certificate, signed by a CA your investigators' browsers trust. Self-signed certificates won't work. That's Chrome's rule, not ours.

1. Choose a DNS name for the server and point it at the IP address the server will run on.
2. Issue the certificate from your CA as `server.crt` and `server.key`, PEM encoded.
3. Make a directory for the server on the host: `mkdir /data/ubikron-server`
4. Copy in the `docker-compose.yml` we give you.
5. Make a `certs` subdirectory and copy `server.crt` and `server.key` into it.
6. In the server directory, create a file called `.env` (note the dot) with your settings and passwords. Your DNS name goes in `S3_PUBLIC_URL` (followed by `/cdn`), `ZITADEL_PUBLIC_URL` and `ZITADEL_EXTERNAL_DOMAIN`, and your organisation identifier in `MIMIC_ORG_NAME`. Use your own secrets, not these:

```
S3_PUBLIC_URL=https://ubikron.acme.com/cdn
S3_PUBLIC_PORT=8333
JHIPSTER_REGISTRY_PASSWORD=f843f4972db8cbc2
ELASTIC_PASSWORD=4fa045782eaae8a4
POSTGRES_PASSWORD=4ff403f10dbd7372
RABBITMQ_PASSWORD=e3e65455710b715d
STORAGE_ADMIN_PASSWORD=143f3287b4628df2
STORAGE_ACCESS_KEY=36a0752ec021d626e2fc
STORAGE_SECRET_KEY=a4cff31f934684a5d8adce51f4ad8092786ea89b
WUD_ADMIN_PASSWORD=3eb906d8bc1d4656
JWT_BASE64_SECRET=R9gVF5Sg/s3axdeI7tZmcWdlAdb+5geqzJ0X87OTuheA3vhrzy7rQ41qG4eaw6h++WaMZLqUbXndtKM
y8Q17eg==
ZITADEL_MASTERKEY=ByohDPXTT4VTzKyxhMnBdTuF6GzH5aGf
ZITADEL_DB_PASSWORD=H8QfvBGGsrCKkIkETxOuaTP5
ZITADEL_SETUP_PASSWORD=kVMi6SDm!S8XH1Cf0oVIataDpqjzAJl93
ZITADEL_PUBLIC_URL=https://ubikron.acme.com
ZITADEL_EXTERNAL_DOMAIN=ubikron.acme.com
ZITADEL_EXTERNAL_PORT=443
ZITADEL_EXTERNAL_SECURE=true
MIMIC_ORG_NAME=acme-corp
MIMIC_SERVER_KEY=servk_tkfiQqRTMCs9AG3IC5vq4bgXOMJ_Yf246zrnef5Fh7o
MIMIC_SECRET_ENCRYPTION_KEY=vrqvCvitCxKYvQkV8hG4ggcOdsJp3wS2DEbHn0dOwRU=
UBIKRON_ADMIN_PASSWORD_HASH=JDJhJDEwJGprSjVDOVMycjByOEkxRzVBak9lOVRVY3hwaUxxQ242NTVKMUNja3R5YjljY
3gwbzh2c2tG
```

Generate every secret yourself:

Value	Make one with
The `_PASSWORD` values	`openssl rand -hex 8`
`STORAGE_ACCESS_KEY`	`openssl rand -hex 10`
`STORAGE_SECRET_KEY`	`openssl rand -hex 20`
`JWT_BASE64_SECRET` : Base64, at least 256 bits	`openssl rand -base64 64`
`MIMIC_SECRET_ENCRYPTION_KEY` : Base64, 32 bytes	`openssl rand -base64 32`
`ZITADEL_MASTERKEY` : exactly 32 characters	`openssl rand -hex 16`
`MIMIC_SERVER_KEY` : `servk_` and 32 random bytes	`echo servk_$(openssl rand -base64 32 | tr '+/' '-_' | tr -d '=')`
`UBIKRON_ADMIN_PASSWORD_HASH` : the admin password as a bcrypt hash, Base64 encoded	`docker run --rm httpd:2.4-alpine htpasswd -nbBC 10 "" 'your-password' | tr -d ':\n' | sed 's/^\$2y/$2a/' | base64 -w0`

7. Start the server: `docker compose up -d`

```
$ ls -la /data/ubikron-server/
drwxr-xr-x  certs/
-rw-r--r--  docker-compose.yml
-rw-r--r--  .env
drwxr-x---  volumes/

$ ls -la /data/ubikron-server/certs/
-rw-r--r--  server.crt
-rw-r-----  server.key
```

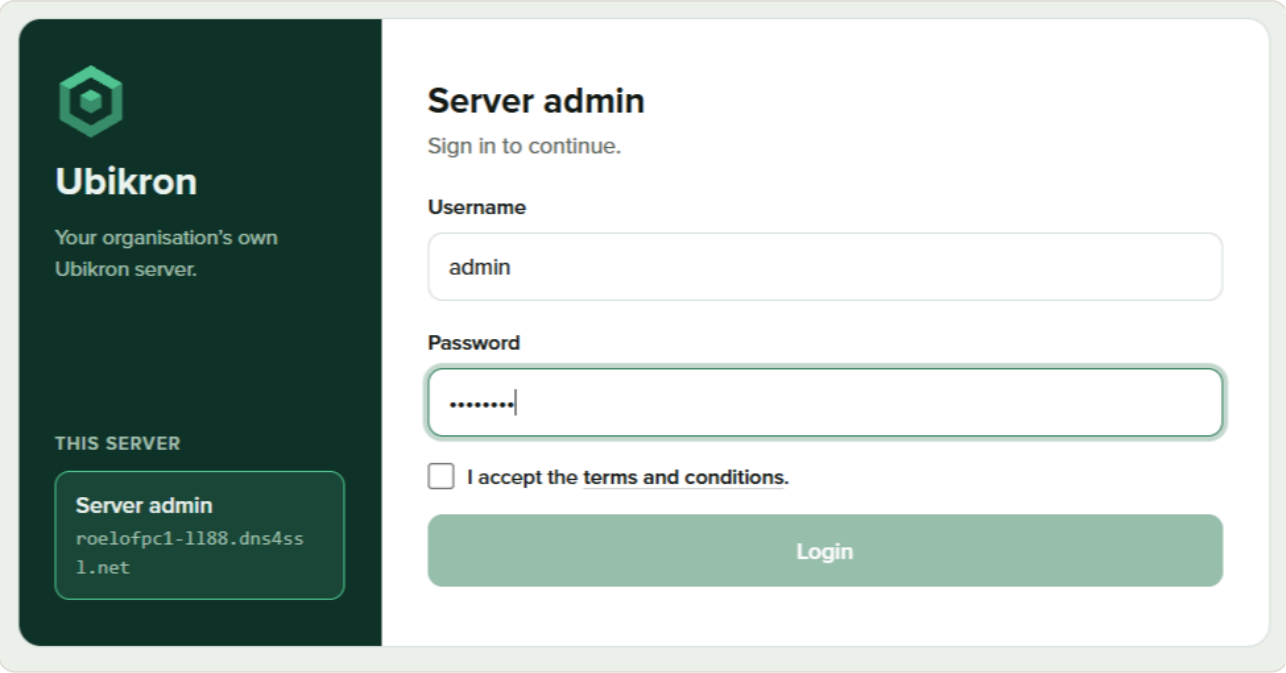
The first start takes time. The services wait for each other, and the logs fill with warnings and errors while they do. That's normal.

When it's up, open the admin interface in your browser. There should be **no** certificate warnings. If there are, the extension won't connect.

6. Administration

Signing in

Open the admin interface at the address the installer gave you. Sign in as **admin** with the password you chose during the install, and accept the terms and conditions.

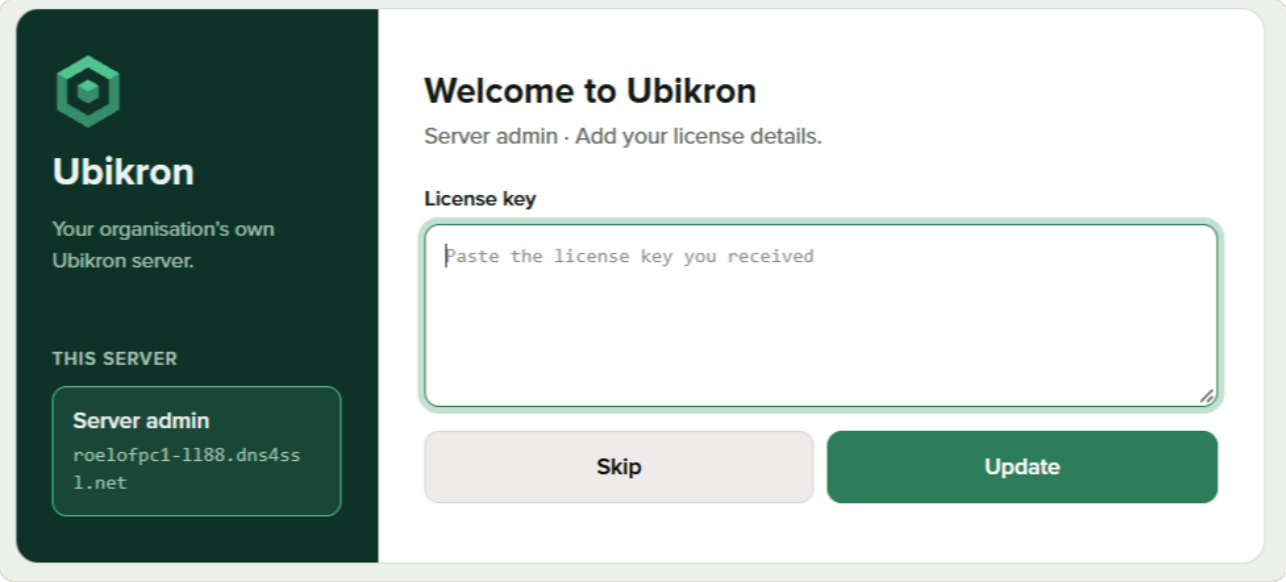


The admin sign-in. The panel on the left shows which server you're on.

Mimic is at `/mimic/` on the same address, for example `https://test-pb56.dns4ssl.net/mimic/`, with the same login.

The license

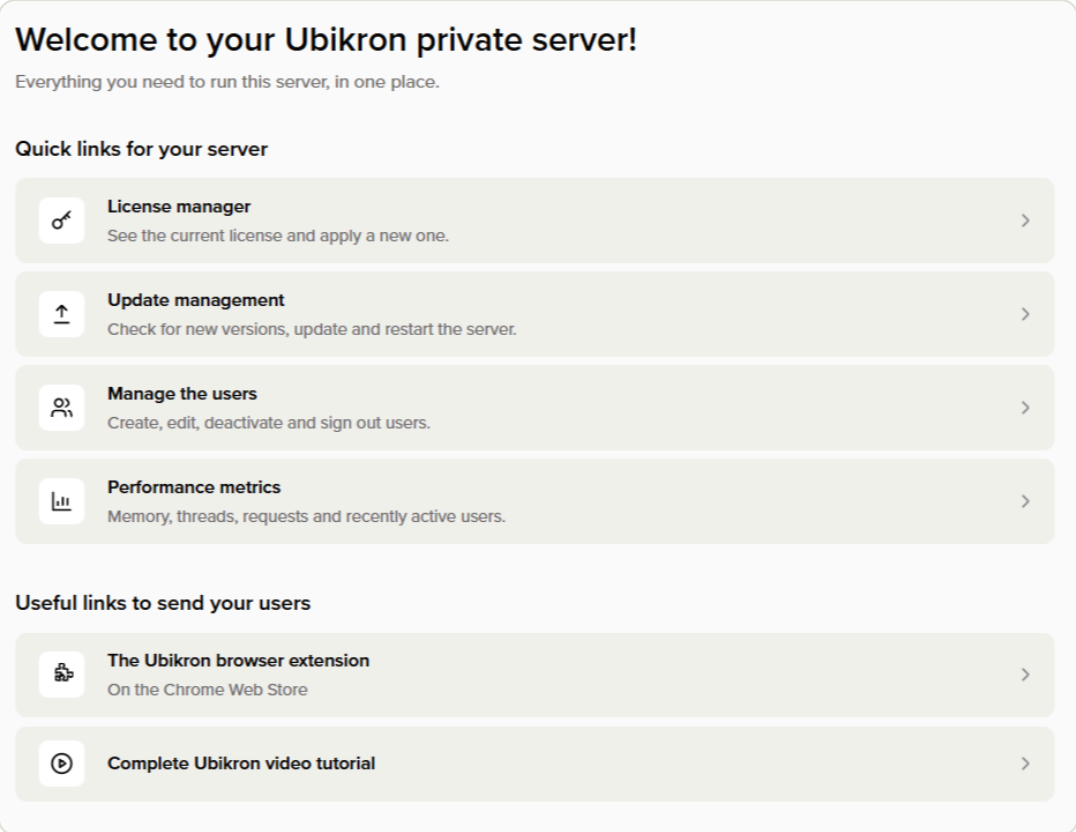
Next you're asked for a license key. No key yet? Click **Skip**. You get the free Try server, shown as Free on the license page: 1 user and 2 projects, signing in with your existing Ubikron license. Enough to see whether it's for you.



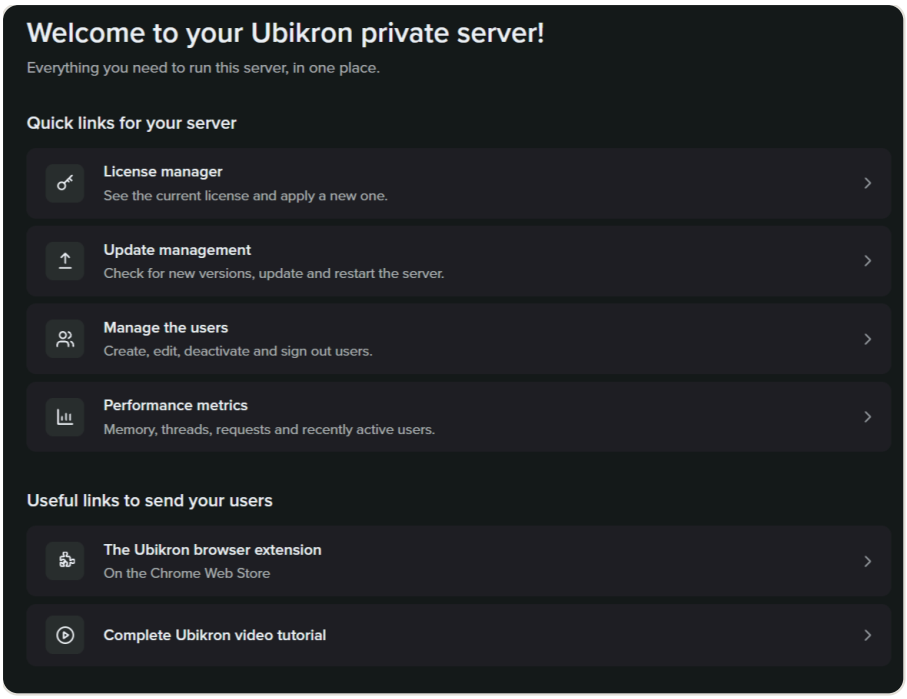
Paste your license key, or skip it for now.

The overview

Then you're on the overview, with links to everything that follows, and links to send your users: the extension on the Chrome Web Store and the video tutorial. The sidebar has the same sections. The admin screens come in light and dark.



The overview.

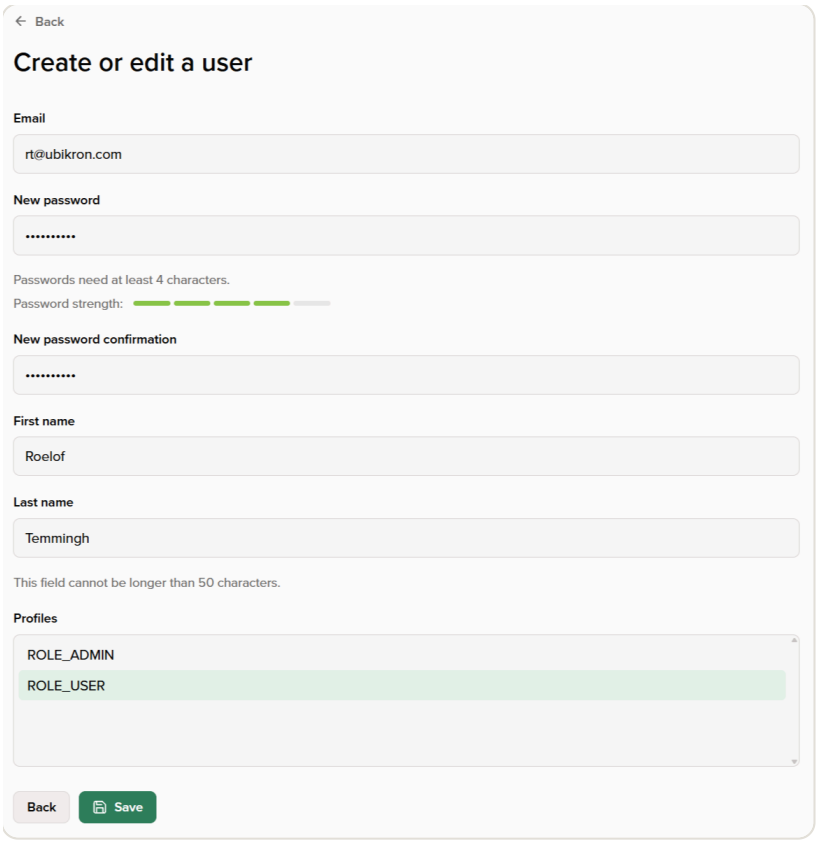


The same screen in dark mode.

Adding users

First, create the user account you'll investigate with. The admin account only runs the server. Click **Manage the users**, then **Create a new user**, fill in the details and click **Save**:

- **Email**: an identifier only. The server never sends email, so a dummy domain such as `analyst@company.local` is fine.
- **Password**, twice.
- **First and last name.**
- **Profile**: ROLE_USER for investigators, ROLE_ADMIN for people who run the server.



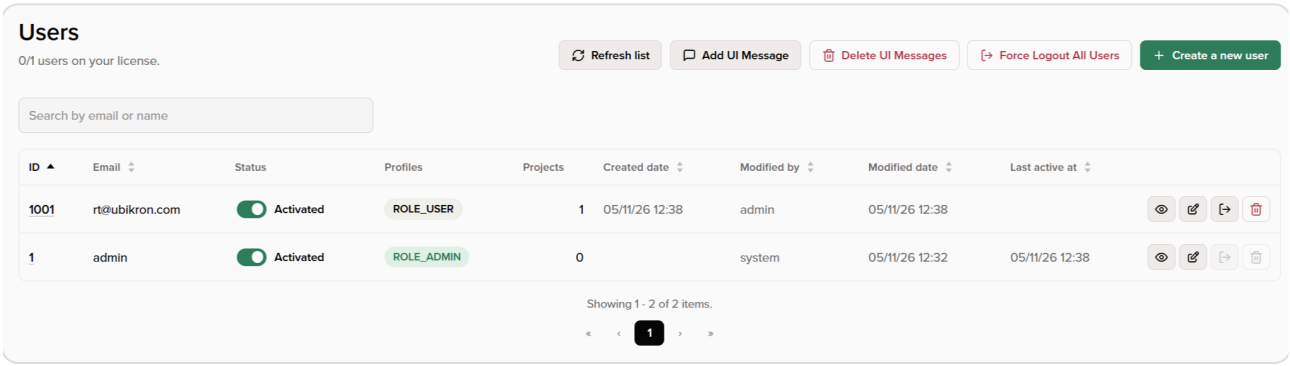
Creating a user.

Saving creates a default project for the user, so it takes a few seconds. The user then appears in the list.

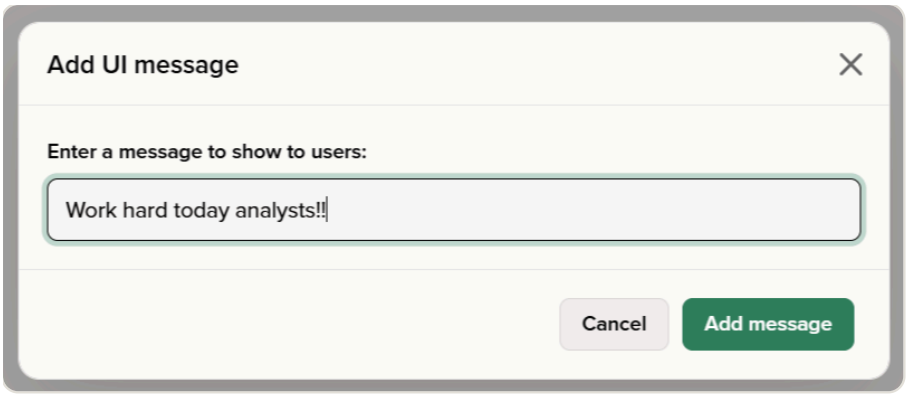
The user list

The list shows each user's profile, projects, and when they were created, changed and last active. The buttons on each row view, edit, sign out or delete that user. Above the list:

- **Add UI Message** shows a message to all your users, for example a maintenance notice. **Delete UI Messages** takes it down.
- **Force Logout All Users** signs everyone out, for example before an update.



The user list. The line under the title shows how many users your license allows.

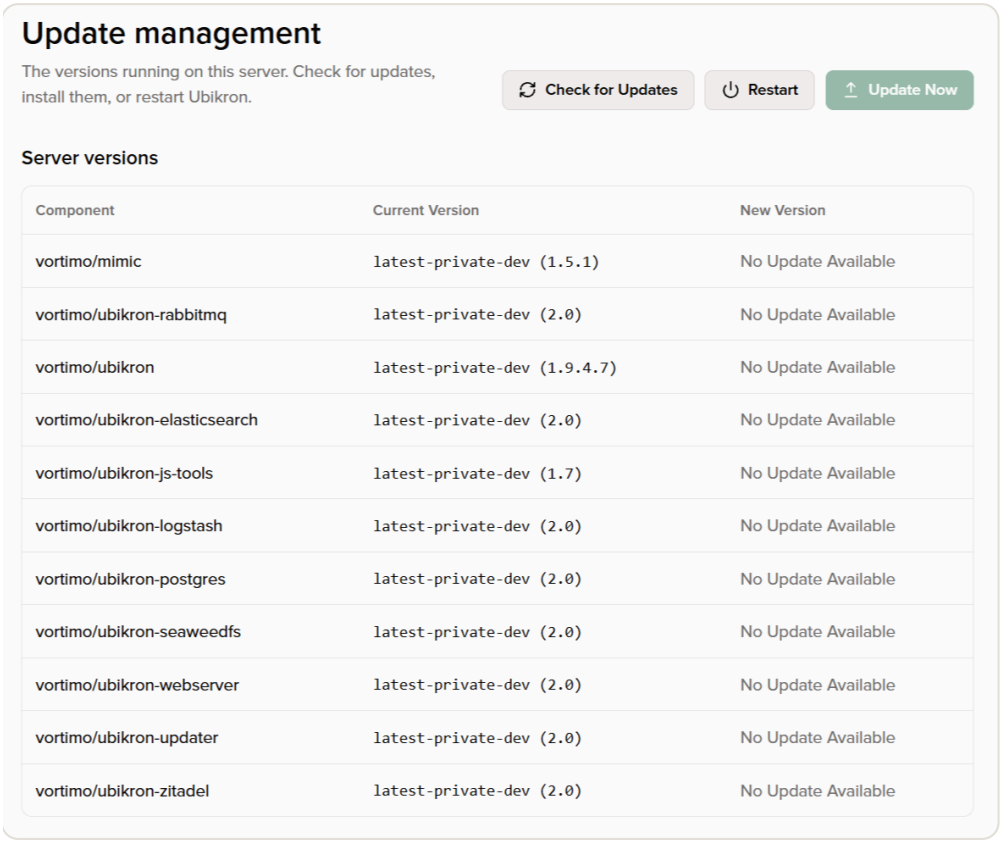


Adding a message for your users.

Updating the server

A container checks Docker Hub every hour for updates to any part of the server. When there is one, your users are told in the extension and asked to tell you, since you'll rarely have reason to sign in to the admin. You're told too when you next sign in.

Go to **Update Management**. It lists every component, its version, and whether there's a newer one. **Check for Updates** refreshes the list, **Update Now** installs what's new, and **Restart** restarts Ubikron.



Every component of the server and its version.

> An update takes a while, and the server is unavailable to your users meanwhile. The admin screen may show errors. That's normal: reload it after a minute.

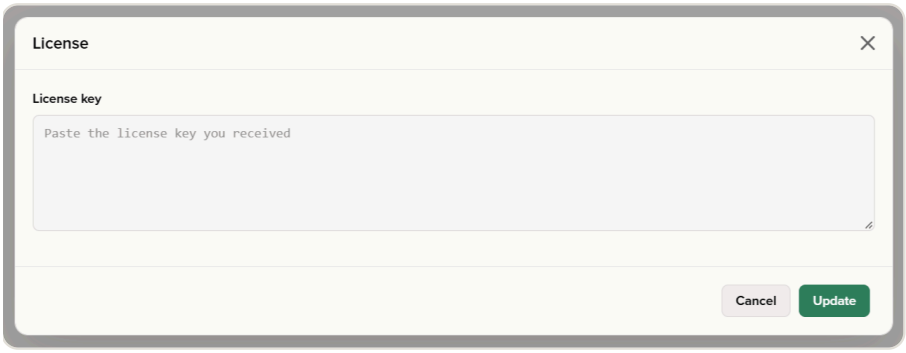
Entering a license key

Go to **Licensing** to see the current license, with bars showing how much of it is in use.

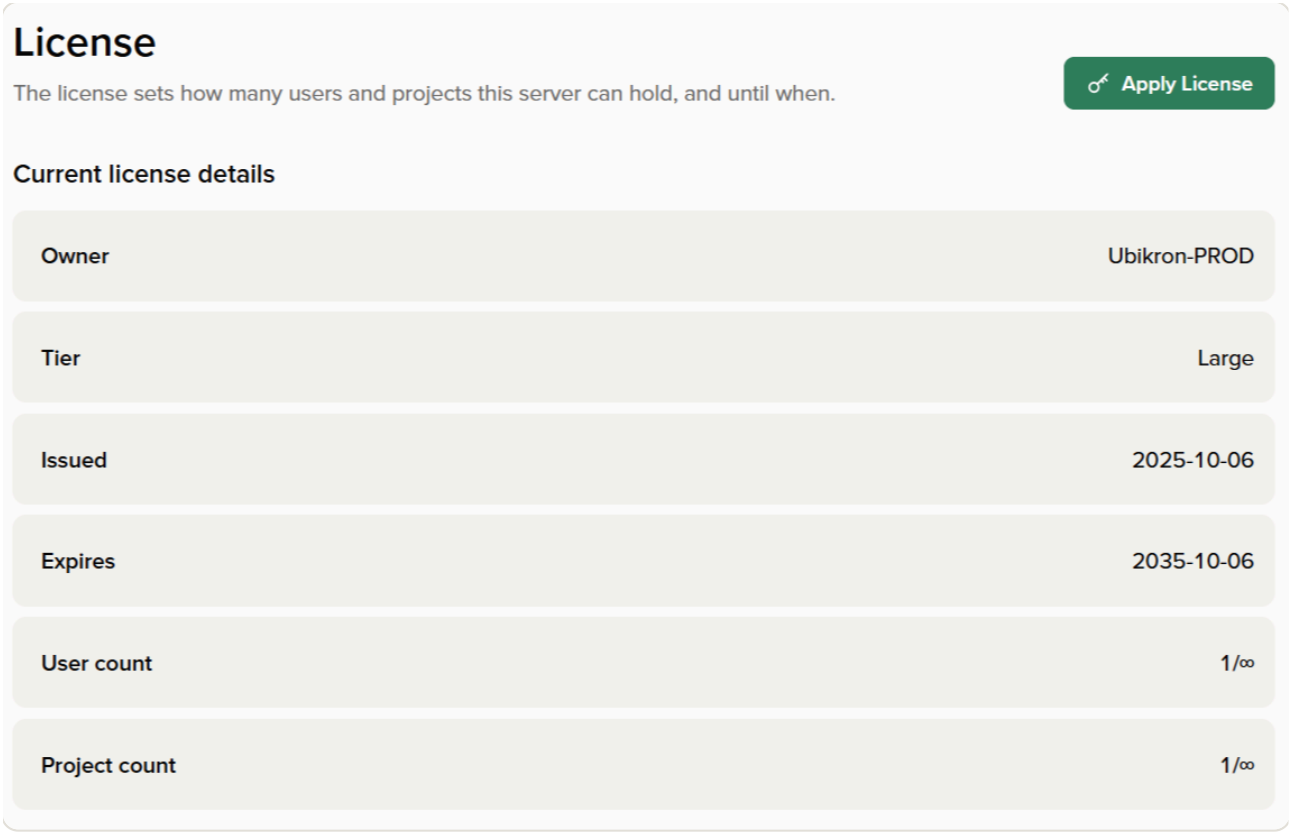


The free license: 1 of 1 users, 1 of 2 projects.

Click **Apply License** and paste the key you received. The license details appear below it: owner, tier, issue and expiry dates, and how many users and projects it allows. If they're right, click **Update**.



Paste the key.

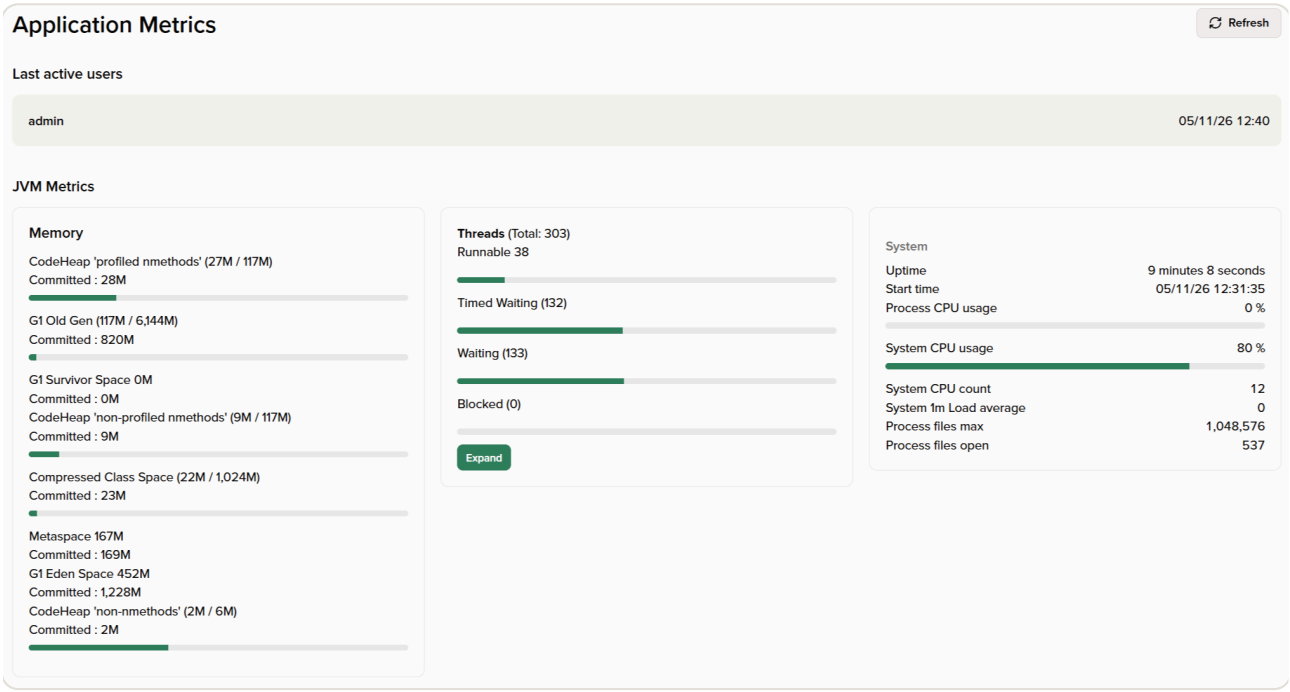


A license applied.

If a license runs out, everyone can still sign in and get to their data, but nobody can add projects or users until you renew.

Metrics

Metrics shows who was active recently, and the server's memory, threads, CPU and uptime.



Performance metrics.

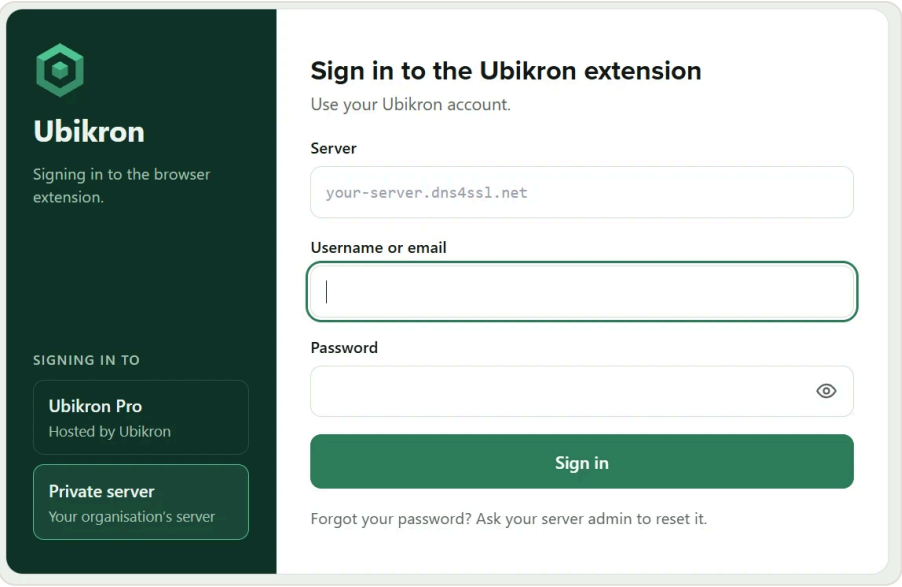
Changing the admin password

Under **Account**, click **Password**. Enter the current password and the new one twice. Choose a strong one: we don't enforce rules on administrators.

7. Connecting the extension

With the server running, a license in place and a user created, your investigators can sign in.

1. Install the Ubikron extension from the Chrome Web Store if it isn't installed.
2. On the sign-in screen, find **Private Server** at the bottom and click **Login**.
3. The screen turns from red to **green** and asks for a server address, email and password.
4. Enter your server's **DNS name**, for example `test-pb56.dns4ssl.net`. For a local install, use `127.0.0.1` or `localhost`.
5. Enter the **email and password** of the user you created.
6. Click **Login**.



Signing in to a private server.

To go back to our server, click **Public Server** on the sign-in screen. The extension remembers both.

8. Troubleshooting

Forgotten admin password

1. Go to the server's install directory and open the `reset-password` subdirectory.
2. Create a file called `reset-admin.txt` in it. Empty is fine.
3. Wait a few minutes. The server checks for it now and then.
4. The password is now **admin**. You'll set a new one when you sign in.

```
$ cd /data/ubikron-server
$ touch reset-password/reset-admin.txt
```

Mac says "Operation not permitted"

macOS couldn't check the installer's signature with Apple, usually because of a weak or missing internet connection. Use the PKG installer, which verifies offline. See Installing on a Mac.

The containers take ages to start

The first start is slow. The services wait for each other and the logs fill with warnings while they do. Give it a few minutes.

Certificate warnings in the browser

The extension won't connect while there are any. Use a certificate your browsers trust, not a self-signed one.

Removing everything

Delete the install directory. That's where all the data is. Removing the Docker containers, images and volumes alone leaves it in place.

Still stuck?

See ubikron.com/help, or tell us what you're seeing at ubikron.com/contact.