

Uplivra is in beta and online purchasing is paused. **Apply to test it:** testers get a license on request and 10% off when purchasing opens.

INSTALL GUIDE · NETWORK PRO

Secrets vault

Store the passwords, keys and tokens your team needs in one encrypted, audited place; let Uplivra change device passwords on a schedule or after each use; and point device logins at the vault.

Uplivra Technologies LLC · Guide for Uplivra 26.10 · Updated 2 October 2026 · Latest version:
<https://uplivra.com/guides/secrets-vault.html>

What it's for

Break-glass admin passwords, Wi-Fi keys, API tokens, license keys, certificates and notes, kept separate from the device logins Uplivra uses for monitoring.

Open it under **Network > Secrets vault** (Network Pro). **Add an item** opens a wizard with five short steps:

1. what it is;
2. the value (typed, or a strong one made for you);
3. which devices it opens;
4. whether Uplivra should change it regularly;
5. who may see it.

How it's protected

Every value sits inside three locks, each a different 256-bit key (AES-256-GCM, an authenticated cipher, so any change to stored bytes is caught):

1. **The value's own key.** Every version of every value gets a new random key.
2. **The folder key.** That key is locked with the key of the folder the item is in. Each folder has its own. Items outside any folder skip this step.

3. **The vault key.** Folder keys are locked with the vault key. It's in `secret-vault.key` in the server's data folder: readable only by the service account on Linux, and wrapped with DPAPI on Windows. It's never in the database, so a copy of the database alone opens nothing.

Other protections:

- **Values can't be moved.** Each value is bound to its item and version, and each folder key to its folder, so a stored value copied elsewhere won't open.
- **Values aren't shown by default.** Nothing appears on a page until someone allowed to reveal it clicks **Reveal** and gives a reason. The value hides itself again after a minute, and a copy is cleared from the clipboard after 30 seconds.
- **Everything is recorded:** each reveal, copy, change, rotation, check, check-out, application fetch and use by a device login. The record is in the item's history and in the hash-chained audit log, and it can be exported.

Replacing keys:

- **A folder key:** open the folder, **Replace the folder key**. Every value key in the folder is re-locked with a new folder key in one step (no value is decrypted), and the old folder key is gone.
- **The vault key: Vault history > Replace the vault key.** Only the folder keys (and values outside folders) are re-locked, so it's quick however big the vault is. The old key file is deleted once nothing uses it.

Back up the server's data folder with the database: Uplivra's own encrypted backups include the vault key.

Who may see what

Roles give four vault permissions:

- **see** the vault (names and history, never values);
- **reveal** values;
- **manage** items;
- **change passwords on devices and approve check-outs.**

Folders narrow that down further (next section).

Check-out: an item can require a check-out before anyone sees it, for a set time, and only one person has it at a time. With **Change the password after each check-out**, a password someone has

seen stops working once they check it back in, or once the time runs out. With the Access Control module, a second person approves each check-out; nobody can approve their own.

Folders and who's in them

A folder groups items and decides who may use them. Open a folder from **Secrets vault > Folders**.

- **No members:** the folder is open to roles. Anyone whose role lets them see or reveal vault items can do so here.
- **With members:** only the people and groups you add get in. For each one, tick what they may do:
- **See the items** (names and history, never values);
- **Show, copy and check out values;**
- **Add, change, rotate and delete items;**
- **Approve check-outs;**
- **Change who's in the folder.**

A member also needs the matching permission in their role. For example, "Show values" in a folder still needs **Reveal and copy secret values** in the person's role. People outside the folder don't see its items at all, not even in search or history.

Add yourself first with **Change who's in the folder**. Uplivra won't let the last person who can manage members leave, so a folder is never locked for good.

Approval for the whole folder: with Access Control, tick **Every check-out in this folder needs a second person**.

Old values

Each new value is kept as a new version. A folder sets how many old values to keep (10 unless you change it) and, optionally, how many days to keep them. The current value is always kept. A failed rotation's value is kept as "failed", so it's never lost.

Checking passwords still work, and reconcile

For an item changed on a device, tick **Check it still works every N days**. Uplivra logs in to the device with the stored value and changes nothing. If the login fails (someone changed the password on the device by hand), the item shows the problem and an alert opens.

To fix it, give the item a **reconcile login**: a stronger device login, such as the device's main admin. **Reconcile** uses it to set a new password, logs in with that password to prove it, and only then saves it. With **reconcile automatically**, a failed check is fixed without anyone stepping in. The alert closes once the value works again.

Who can get to what

Secrets vault > Who can get to what lists every person and application that can reach vault items, folder by folder. It shows how they got access (their role, membership of the folder, or an application token) and how often they used it in the last 90 days. Lines that can show values but weren't used are flagged, so you can take that access away. Export it as CSV for an access review or an audit.

Applications (scripts)

A script or program can fetch a password from the vault instead of keeping it in a file. Under **Secrets vault > Applications**, add one:

- **Folders**: it can only read items in the folders you pick.
- **Allowed from**: only from the addresses or ranges you enter.
- **Token**: shown once. Uplivra keeps only a fingerprint of it.

The script then asks:

```
curl -s -H "Authorization: Bearer YOUR-TOKEN" "https://your-uplivra/api/v1/vault/secret?name=Backup%20share%20password"
```

The answer is JSON with the name, user name, value and version. Every fetch is recorded like a reveal, as `app:NAME`. Items that need a check-out or approval are never given to applications. Turn an application off, or delete it, and its token stops working at once.

Rolling passwords on devices

Set **Changing it** to **Change it on a device automatically**, then pick:

- the device;
- its kind (Cisco IOS, NX-OS, ASA, Arista, Junos, Aruba CX, ProCurve, FortiOS, MikroTik, Huawei, Dell OS10, Ruckus, Linux or Windows);

- the SSH device login that makes the change.

The change is made in this order, so a password is never lost:

1. The new password is saved first, encrypted, as **pending**.
2. Uplivra sets it on the device.
3. Uplivra logs in with the new password.
4. Only when that login works does the new password become current.

If the login fails, Uplivra puts the old password back and keeps the failed one, so you can still see what was set. Passwords are never shown in the command output Uplivra keeps.

Palo Alto, SonicWall and others that can't be changed safely over SSH get a reminder instead. Use **Rotate now** once while you watch before you rely on the schedule.

Device logins from the vault

Under **Settings > Device logins**, choose **Password from the vault** for a login. The login then always uses the item's current value: rotate the item and every check using that login follows.

HashiCorp Vault and CyberArk

Already keep passwords there? Add the external vault under **Secrets vault > External vaults**:

- **HashiCorp Vault**: KV version 2, signing in with a token or AppRole.
- **CyberArk**: the Central Credential Provider, with an application ID, a safe and an optional client certificate.

Then point an item at a path or account. Uplivra fetches the value each time over HTTPS and never stores it. Your Vault or CyberArk software and license stay yours; nothing of theirs is included in Uplivra.