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 · COMPLIANCE & EVIDENCE

Compliance and evidence

How to give each control an owner and a scope, link evidence to devices, save log messages and web page screenshots as evidence, open tickets from findings, and run access reviews that repeat on their own.

Uplivra Technologies LLC · Guide for Uplivra 26.10 · Updated 28 September 2026 · Latest version: https://uplivra.com/guides/compliance.html

What you need

- The **Compliance & Evidence** module on your license. Everything on this page is part of it.
- The **Compliance › See controls, evidence and findings** permission to look, and **Collect evidence, record findings and reviews** to change things. Taking web page screenshots needs its own permission, **Set up and take web page screenshots as evidence**, because it keeps sign-ins for those pages.
- Optional extras, each explained below: **Log Intelligence** (or Network Pro's event viewer) for log extracts, **headless Chromium or Chrome** on the Uplivra server for screenshots, the **Service Desk** module or **ITSM Integration** for tickets, and an **email alert destination** for review reminders.

Evidence can't be edited or deleted once it's saved. Every item has a SHA-256 hash and is chained to the one before, so a change made outside Uplivra shows on the Compliance page.

Give each control an owner and a scope

Open a control (**Compliance**, then click it) and use **Owner and scope**:

- **Owner**: the person responsible for it. It must be someone who can sign in to Uplivra. New findings on the control go to the owner unless you name someone else.
- **Covers**: **all devices** (the default), or only **some sites**, **some device groups** (the ownership groups from Vulnerability Scanning) or **devices with some tags** (for example `pci`).

The scope is used everywhere for that control:

- the **automated check** only looks at devices in scope, and says how many that is;
- the **records** saved with the evidence (device lists, configuration backups, certificates…) only list devices in scope;
- evidence and findings can only be linked to devices in scope;
- a **log extract** keeps only messages from devices in scope.

My controls: on the Compliance page, **Show only my controls** lists the controls you own. On **Findings**, tick **Only my controls and findings** to see findings on your controls and findings given to you.

Evidence linked to devices

When you save evidence on a control's page, pick the devices it's about (hold Ctrl or ⌘ to pick several). Uplivra also links devices by itself:

- a **screenshot** of a device's page is linked to that device;
- a **log extract** is linked to the devices the messages came from;
- when an **automated check fails**, the saved result is linked to the devices behind the failure (for example the devices without a recent configuration backup).

Each device's page shows its **Compliance evidence** and open findings. **Compliance › Evidence** lists everything, filtered by control, device or kind. Open an item to see its hash, where it came from, and its devices; you can link or unlink devices there. Linking changes where evidence shows, never the evidence itself.

Save log messages as evidence

Search the logs as usual (**Logs**), then click **Save as evidence**:

1. Pick the control (for example **UPL-08 Watch for failed sign-ins**) and, if you like, a title.
2. Uplivra keeps the matching messages, **newest first, up to 1,000**, in a ZIP with: - `messages.csv`: the messages, with time, sender, device, site and program; - `README.txt`: the search and filters, the exact time range searched, how many messages matched, which site and **collectors received them**, the **SHA-256 of messages.csv**, and when the originals leave the log store.

Retention: Uplivra deletes log messages after the number of days set under **Settings › Logs** (7 days in Network Pro's event viewer). The page and the README tell you when the originals behind the

extract go. **The extract itself is evidence**: it's kept with the rest of the evidence and doesn't expire with the logs.

Screenshots of web pages as evidence (optional)

Uplivra can open a device's or system's web page, such as a firewall's admin page, sign in, black out what shouldn't be kept, and save a picture as evidence.

Install Chromium on the Uplivra server

This is **optional**: everything else works without it. Uplivra looks for Chromium or Chrome every minute, so no restart is needed after installing.

Server	Command
Ubuntu or Debian	`sudo apt install chromium` (Ubuntu installs the snap), or Google Chrome from google.com/chrome
Red Hat, Rocky or Alma	`sudo dnf install epel-release && sudo dnf install chromium`
Somewhere else	Set `UPLIVRA_CHROME=/path/to/chrome` in the server's environment and restart Uplivra

Compliance › Screenshots says whether it was found, and which version.

Add a page

Compliance › Screenshots › Add a web page:

- **Page address**, for example `https://192.168.1.1/`, and the **control** the screenshots are evidence for. Pick the **device** to link them to.
- **Accept the device's own certificate** if the page uses a self-signed one.
- **Sign in first** (optional, for simple sign-in forms): a user name and password, and CSS selectors for the user name field, the password field and the sign-in button (leave the button empty to submit the form). **Then open** can go to another page on the same address after signing in. Use a **read-only account**.
- **Black out**: CSS selectors (one per line, such as `#serial-number`) and fixed areas as `x,y,width,height` in pixels. They're covered before the picture is taken, so they never reach

the evidence. A selector that matches nothing is noted with the screenshot.

Then click **Take a screenshot**. The picture is saved as evidence (PNG) with a line across the bottom showing the address, the time (UTC) and who took it; its SHA-256 and time are shown with it on the evidence page.

How the password and the network are protected

- The password is **encrypted with the server's secrets key**, never shown again, never logged, and only sealed for that page's address: change the address and you must type it again.
- It's only typed into the page when the page is **still on the target's own address**. If the page sends the browser somewhere else first, Uplivra stops without typing it.
- Every connection the browser makes goes through a small filter inside Uplivra that only lets it reach **private addresses** (10.x, 172.16–31.x, 192.168.x, 100.64–127.x and IPv6 unique local). It can't reach the internet, the Uplivra server itself, or link-local and cloud metadata addresses. Anything the page tried to reach and couldn't is listed with the result.
- The browser runs headless with a fresh, empty profile each time, which is deleted afterwards; no debugging port is opened.
- The page must be reachable **from the Uplivra server**. A server in the cloud usually can't reach your office network; use the log extracts or upload a screenshot instead.

Findings that open tickets

On **Findings**, an open finding has **Open a ticket in**:

- **Service Desk** (Service Desk module): a ticket in the Compliance category, priority from the finding's severity, linked to the finding's device and to the finding;
- a connected **ticketing system** (ITSM Integration: ServiceNow, Jira Service Management, Freshservice, Zendesk or a webhook, set up under **Settings › Ticketing**): an incident with the finding's details and a link back.

The finding shows the ticket's number and state. It works both ways:

- **Resolving the finding** resolves the ticket (Service Desk, or the other system through its API; a webhook gets a `compliance.finding.resolved` event).
- **Closing the ticket** shows on the finding. Service Desk tickets are noticed straight away; ServiceNow, Jira, Freshservice and Zendesk are asked every hour (webhooks can't be asked). A finding you added by hand is resolved with its ticket; a finding from an automated check stays with the check and resolves when the check passes.

Opening, resolving and any problem talking to the other system are recorded in the audit log.

Access reviews that repeat

Compliance › Access reviews › Start a review:

- **Repeats**: once, every month, every quarter or every year. The next review is started automatically, with the same reviewers, when this one is **completed** or reaches its **due date**, whichever comes first, and only once.
- **Second reviewer**: nobody decides their own access. The reviewer's own account is decided by the second reviewer, and Uplivra refuses a decision anyone makes about their own account.
- **Reminders**: the reviewers get an email a week before the due date, and every 3 days until the review is done. Emails go through your email alert settings (**Settings › Where alerts go**); without them, no reminders are sent.
- **Overdue** reviews are marked on the reviews list and the Compliance page, and raise an alert.

Completed reviews are saved as evidence for **UPL-05 Review who has access**.