How to Use Passkeys at Wey Valley Radio

A step-by-step guide for the WVR team

VERSION 1.0 · JUNE 2026

This guide picks up where *Passkeys: What They Are and Why They Matter* leaves off. It explains how Wey Valley Radio's sign-in works, what to expect when you set up your account, and how to register and look after your passkeys — including the steps for each type of device.

Contents

1. How Wey Valley Radio sign-in works

Wey Valley Radio uses a single, secure sign-in for its online tools, run by software called **Kanidm**. It lives at:

https://kanidm.weyvalleyradio.uk

Think of it as the station's front door. Rather than every WVR service having its own separate password, you sign in once, here, with your passkey — and it lets you through to the station systems you're allowed to use. This is called **single sign-on**, and it means:

- one identity to look after, not a dozen scattered logins;
- passkeys instead of passwords, so there's nothing to be phished or leaked;
- the team can grant or remove access centrally if your role changes.

You'll either be sent to kanidm.weyvalleyradio.uk automatically when you open a station service, or you can go there directly.

> **A note on the word "passkey":** Kanidm uses "passkey" to mean *any* cryptographic device login — a hardware key, Windows Hello, Apple Face/Touch ID, or a passkey held in 1Password or LastPass. Whichever you choose, the station system treats it as your passkey. Section 6 covers each type.

---

2. Setting up your account for the first time

You don't create a WVR account yourself — the team sets it up and sends you a one-time **enrolment link** (sometimes shown as a QR code) so you can add your own passkey. Here's exactly what to expect.

What you'll receive

A link that looks like this:

https://kanidm.weyvalleyradio.uk/ui/reset?token=XXXXX-XXXXX-XXXXX-XXXXX

Two things to know about it:

- It's **time-limited** — at Wey Valley Radio the link is valid for **one hour**, so open it soon after it arrives and set aside a few minutes to finish.
- It's **single-use** — once you finish, the link stops working. That's normal, and a good security feature.

If the hour runs out before you're done, the link simply expires — just ask the team for a fresh one and start again.

(If you were given just the code rather than a full link, go to https://kanidm.weyvalleyradio.uk/ui/reset and type it in.)

Step by step

1. **Open the link** on the device you'd like to register first — your phone or laptop is fine.
2. You'll see your name and a credential setup screen. Choose **Add Passkey**.
3. **Give the passkey a name** you'll recognise later — e.g. "Jane's iPhone" or "Jane's YubiKey." It's just a label so you can tell your devices apart.
4. Your device or browser then takes over with its usual prompt — **Face ID, fingerprint, a Windows Hello PIN, or a tap on your hardware key.** (The exact prompt depends on the device — see Section 6.)
5. The passkey appears in the list. **Now add a second one if you can** — see the box below.
6. If the screen offers it, you can also set a **password plus an authenticator-app code** as a backup method. If it's offered, it's a sensible safety net.
7. **Important: choose Submit / Save to finish.** Nothing is stored until you do — and once you do, the enrolment link is used up.

> **WVR's strongest recommendation — add more than one passkey now.** While the setup screen is open, register at least two: for example your phone *and* a hardware key, or your laptop *and* your phone. Just keep choosing **Add Passkey** before you save. This single habit is the best protection there is against being locked out if a device is lost or broken.

---

3. Signing in day to day

Once you're set up, signing in is quick:

1. Open the station service, or go to **https://kanidm.weyvalleyradio.uk**.
2. **Enter your WVR username** (the team will tell you what this is) and continue.
3. Select **Use passkey**.
4. Your device prompts you for **Face ID, fingerprint, PIN, or your hardware key** — confirm, and you're in.

A couple of things worth knowing:

- **The extra "Use passkey" button is normal.** Some browsers need one deliberate click before they'll start a passkey prompt, so Kanidm shows a **Use passkey** button. Clicking it is expected — it isn't a fault.
- **If you registered several passkeys,** your browser decides which to offer and may pick one automatically. In Firefox especially, you might be offered your hardware key when you wanted your phone, or the other way round — just cancel and choose the other.
- **If you set up a password + authenticator-app backup,** you can choose that instead of a passkey when you sign in.

---

4. Adding another passkey later

You'll want to do this when you **get a new phone or laptop**, or when you decide to **add a hardware-key backup** to an account you first set up in a hurry.

Because adding a passkey is a security-sensitive change, it's done through the same kind of one-time link as your first setup:

1. **Ask the WVR team for a new enrolment link** — it takes them only a moment to generate one.
2. Open the link, choose **Add Passkey**, name it, and confirm with the new device.
3. Add any others you want in the same session.
4. **Save** to finish.

Your existing passkeys keep working — this *adds* to them, it doesn't replace them. If you ever want to remove an old device (say, a phone you've sold), ask the team to remove that specific passkey.

> **Tip:** it's far easier to register a device while it's in your hand. When you get a new phone, add it as a passkey straight away rather than waiting until you're locked out of something.

---

5. If you lose a device or get locked out

Don't worry — this is exactly why we ask you to register more than one passkey.

- **If you still have another registered device:** sign in with that as usual, then ask the team to remove the lost one and help you add a replacement.

- **If you can't get in at all:** contact the WVR team. They can clear your old credentials and send a fresh enrolment link so you can set up again. (For security, removing a credential immediately signs out anything that was using it.)
- **If a device is lost or stolen,** tell the team promptly so its passkey can be removed — even if you can still get in by other means.

Because there's no password for anyone to guess, a lost device is far less dangerous than a lost password would be. It's still worth sorting out quickly.

---

6. Registering each type of device

When the Kanidm setup screen says **Add Passkey** and hands over to your device, what happens next depends on the device. These are the common ones. In every case, the "site" or "account" you're registering with is **kanidm.weyvalleyradio.uk**.

> **A note on wording:** exact button text varies a little by device and version. The *steps* are reliable; if a label doesn't match exactly, look for the nearest equivalent.

6a. Physical passkey (hardware security key)

A YubiKey, Google Titan, or similar — a small device you plug into USB or tap via NFC.

When you choose **Add Passkey** and your browser asks where to save it: 1. Choose **Security key** (rather than "this device" or a phone). 2. **Insert the key** into a USB port — or, on a phone, hold the key against the back of the handset for NFC. 3. The first time you ever use a new key, you'll be asked to **create a PIN for the key itself**. Choose one and keep it safe — it protects the key if it's lost. 4. **Touch the gold disc or button** on the key when it flashes. That physical touch proves a real person is present. 5. The key now appears in your Kanidm list (name it if prompted).

To sign in later: enter your username → **Use passkey** → insert or tap the key → enter its PIN if asked → touch the button.

Tips - **Buy two and register both** — one to carry, one kept safe at home as a backup. Losing your only key makes recovery much harder. - A hardware key never touches your computer's storage, so it's immune to malware on the PC — which is why it's the strongest option.

6b. Windows (Windows Hello PIN)

On Windows, passkeys are protected by **Windows Hello** — a PIN, fingerprint, or face login tied to your PC. If you've ever set up a PIN to unlock your computer, you're most of the way there.

Step A — set up Windows Hello (one-time) 1. Open **Settings** → **Accounts** → **Sign-in options**. 2. Select **PIN (Windows Hello)** → **Set up**, and follow the prompts to choose a PIN. 3. If your PC has a fingerprint reader or compatible camera, set up **Fingerprint** or **Facial recognition** here too — it's faster than typing the PIN.

Step B — register the passkey 1. When you choose **Add Passkey** in Kanidm, Windows pops up a **"Save passkey"** box. Choose **This device (Windows Hello)**. 2. Confirm with your **PIN, fingerprint, or face**. Done.

To sign in later: enter your username → **Use passkey** → confirm with Windows Hello.

You can see and remove the passkeys saved on a Windows 11 PC under **Settings → Accounts → Passkeys**.

> **Heads-up:** a passkey saved this way lives on *that PC*. If it's your only one and the PC dies, you'd need the team to help you set up again — which is exactly why we ask you to register a second device (a phone or a hardware key) as well.

6c. Apple — iPhone, iPad, Mac

Apple passkeys are stored in your **iCloud Keychain** and **sync automatically** across every Apple device signed in to the same Apple Account. Register one on your iPhone and it's instantly available on your Mac and iPad.

Step A — make sure syncing is on (one-time) 1. On iPhone/iPad: **Settings** → tap **your name** → **iCloud** → **Passwords** (or *Passwords and Keychain*) → turn **on**. 2. On Mac: **System Settings** → **your name** → **iCloud** → **Passwords** → **on**.

Step B — register the passkey 1. When you tap **Add Passkey** in Kanidm, a panel offers to save it to iCloud. 2. Confirm with **Face ID** or **Touch ID**. That's it — it's now on all your Apple devices.

To sign in later: enter your username → **Use passkey** → confirm with Face ID / Touch ID.

On a non-Apple device (e.g. a friend's Windows PC): choose **Use passkey → use a phone**, and a **QR code** appears. Scan it with your iPhone camera and confirm with Face ID — the passkey stays on your phone; it just authorises that one login.

You can see, rename, or remove passkeys in the **Passwords** app on any Apple device.

6d. Bitwarden

Bitwarden stores passkeys in your encrypted vault and syncs them across **every** device — Windows, Mac, Android, iPhone. It's open-source, and its **free** plan already includes passkey storage, so it costs nothing to use for this.

One-time setup 1. Create a free Bitwarden account, then install the **Bitwarden browser extension** (Chrome, Edge, Safari, Firefox) and, if you like, the **mobile app**. 2. Sign in to Bitwarden and unlock the extension.

Register the passkey 1. When Kanidm shows **Add Passkey**, Bitwarden offers to **save the passkey to your vault** — accept it. 2. The passkey is stored and is immediately available everywhere you're signed in to Bitwarden.

To sign in later: start the sign-in, and Bitwarden offers the matching passkey — confirm by **unlocking Bitwarden** (Face ID, fingerprint, PIN, or your master password).

Tips - Choose a **long, unique master password** — it's the key to everything in the vault, so make it memorable but strong. - Turn on Bitwarden's own two-step login for the vault, so the vault itself is well protected.

6e. 1Password

1Password stores passkeys in your encrypted vault and syncs them across **every** device — Windows, Mac, Android, iPhone — not just one ecosystem.

One-time setup 1. Install the **1Password app** and the **1Password browser extension** (Chrome, Edge, Safari, Firefox). 2. Sign in to 1Password so the extension is active.

Register the passkey 1. When Kanidm shows **Add Passkey**, 1Password offers a **"Save in 1Password"** prompt — click it. 2. The passkey is stored in your vault and is immediately available on all your devices.

To sign in later: start the sign-in, and 1Password suggests the matching passkey — confirm by **unlocking 1Password** (Face ID, fingerprint, Windows Hello, or your account password).

Tip: 1Password shows a small **passkey icon** in fields where a site supports them — a handy nudge to upgrade older logins too.

Other managers

Other password managers — LastPass, Dashlane and similar — handle passkeys in the same way: when Kanidm shows **Add Passkey**, accept the prompt to save it to the vault, and unlock the vault to sign in later. (We lean towards Bitwarden or 1Password — in LastPass's case partly because of its 2022 data breach — but any reputable, up-to-date manager works.)

---

7. Backup and recovery checklist

This is the part people forget, and the part that matters most.

- **Register at least two passkeys for Wey Valley Radio** — for example a passkey on your phone *and* a hardware key in a drawer. If one is lost, the other gets you in. (See the box in Section 2.)
- **Spread them across different devices.** Two passkeys on the same phone don't help if you lose the phone.
- **Hardware keys: buy a spare** and register both at the same time, then store the second somewhere safe.
- **Add new devices straight away.** New phone or laptop? Ask for an enrolment link and register it while it's in your hand (Section 4).
- **Tell the team quickly** if a device is lost or stolen, so its passkey can be removed.
- **Test it once.** After setting up, sign out and back in immediately, while you still remember what you did. Better to find a snag now than at 11pm when you're locked out.

Stuck on any step? The WVR team is happy to sit down and work through it with you — at the station or over a call.