



The

Broadcasters' Desktop Resource

www.theBDR.net

... edited by Barry Mishkind – the Eclectic Engineer

BDR Password Generator Quick Start

This manual is for the *BDR Password Generator*, which can be [found here to run or download](#). The app is free. If you like it, we invite you to [join the one-time-a-week BDR Newsletter here](#).

[July 2026] With the upcoming requirement to better secure EAS gear (and other equipment), it takes a few moments to get a password that fit the FCC's Order. To get several can take time. Ken Fine's BDR Password Generator will solve this – you can get any number of strong passwords in an instant.

USING THE BDR PASSWORD GENERATOR

Based on the instructions document, here is the basic workflow and quick start.

1. OPEN THE TOOL

- [Save the HTML file PassGen.html](#) to your device.
- Open it in a web browser such as Chrome, Firefox, Edge, or Safari.
- Internet connection is **NOT** needed for running the app. Air-Gapping is encouraged. However, you can run it directly from the download server.
- If it has not already done so, select phone or wider display in the upper right corner.

2. CHOOSE OR CREATE AN EQUIPMENT LABEL

The tool starts with two labels:

- **EAS**
- **STL**

Password for

You can: add new labels – such as a transmitter, automation system, etc - by using the identifier box under the character type selections, and then pressing the **ADD** button.

3. GENERATE A PASSWORD

- Select a label from the dropdown menu.
- Choose whether new passwords contain:
 - Uppercase letters
 - Lowercase letters
 - Numbers
 - Symbols
- Choose the password length – up to 32 characters
- Press **NEW PASSWORD**
- The tool automatically creates a new random password.

New password

Copy

Password for EAS

J1xwDCSfi3nv3SZU

4. APPLY THE PASSWORD

- Click **COPY** to copy the displayed password to your clipboard.

If copying succeeds:

- The button turns teal and shows **COPIED!**
- PASTE** it directly into your equipment's password field or your ledger – **and** the secure place you are saving all your passwords. This might be a file moved to another device or a flash drive.

Password for

EAS

New password

Copied!

If copying fails:

- The button turns red and shows **FAILED**.
- The password is automatically highlighted so you can manually copy it with Ctrl+C, Cmd+C, or a press-and-hold action.
- One caution about the Copy button: the password stays on your clipboard until something replaces it, and Windows clipboard history can keep it around longer than that. After you paste it into your gear and your records, copy something harmless over it and on a shared studio machine, it is recommended you turn clipboard history off.

5. RINSE AND REPEAT

Anytime you need a new password.

- Open the tool.
- The tool will show the existing password if one already exists.
- Select each equipment label at the top.
- Press **NEW PASSWORD**
- Use the displayed password while updating that equipment.

6. VIEWING ALL CURRENT PASSWORDS

The "**The Current Passwords**" section shows the current password associated with each label so you can update one or multiple devices during one session.

Currently set passwords		Wipe device data
EAS	Jul 11 1:02 PM	J1xwDCSfi3nv3SZU
STL	Jul 11 12:48 PM	ticnld0vmIDKFsLY

Note: there is a feature so you can set the number of days when the app will color red and highlight passwords older than the number of days you set.

7. CHANGE A PASSWORD IMMEDIATELY (IF NEEDED)

If you believe a password may have been exposed:

- Select the label.
- Click **NEW PASSWORD**.
- The tool generates a fresh password right away.

8. MANAGE STORED DATA

The BDR Password Generator stores the basic data and current passwords, so they are there when you open the app. You can make changes and delete no longer needed passwords as needed.

- **ADD:** Create a new equipment label.
- **DEL:** Remove a label and its stored password history from that device.

Add

Each label keeps its own password, stored only on this device.

Del

- **WIPE DEVICE DATA:** You can erase all labels and passwords stored by the tool on that device. The link is up above by the Currently set passwords table;

Currently set passwords

[Wipe device data](#)

NOTE! ... clicking on “Wipe device data” restores everything to when you first ran the app.

Important reminders”

1. The passwords are stored only on the device where they were generated. Opening the HTML file on another computer or phone will **not** show the same passwords.
2. If you are not air-gapping the device this is used on – in other words, if your device is directly on the Internet – you might want to “delete” or “wipe” the data AFTER you copy and save it somewhere – a file, perhaps on a flashdrive.
3. We recommend keeping a **separate secure record** of generated passwords, such as in a Key Information binder, password manager or locked password log. This will prevent loss of the passwords should your system crash.
4. This is freeware. There is no warranty. User assumes any and all liability.

- - -

Do you like this app? Please let us know at app@theBDR.net

- - -

Would you like to know when more articles like this are published? It will take only 30 seconds to [click here and add your name to our secure one-time-a-week Newsletter list](#).

Your address is never given out to anyone.

[Return to The BDR Menu](#)