IT APPROVAL PACK

# Dictation Dongle

Production firmware
21 November 2026

A USB keyboard that types what its owner dictates on their iPhone. The phone turns speech into text with Apple's on-device recognition (audio never leaves the phone) and sends the text over an encrypted, bonded Bluetooth LE link to the dongle, which types it at about 70 characters per second. No driver or software on the computer. We do not claim it will get past your controls: approval is your decision, and we tell users to ask you before they plug it in.

## What the computer sees

| | |
|---|---|
| Interface | One HID interface only: class 03, subclass 01 (boot), protocol 01 (keyboard). Device class 0. |
| Nothing else | No serial (CDC) port, mass storage, audio, vendor-defined or other interface. |
| VID / PID | `0x2886` / `0x0056` (decimal 10374 / 86) |
| Strings | Manufacturer "esp32-dictation-keyboard", product "Dictation Keyboard" |
| Serial | Unique per unit, 12 upper-case hex digits from the chip's factory ID (base MAC), e.g. `7CDFA1001234`. Stable across replugs. |

> The VID/PID are the Seeed XIAO ESP32-S3 board's IDs, shared by every such board. Pin allow rules to each unit's serial to approve only the units you have seen.

## What it is not

**Not a mouse jiggler. Not a macro or keystroke-injection device.**

- Types only text its owner has just dictated and the paired phone has sent. Idle, it does nothing: no timers, no stored scripts, no simulated activity, no mouse.
- Sends characters, Enter and Tab. Its only modifiers are Shift and AltGr; never Ctrl, Alt or Command shortcuts, the Windows key, function keys, Backspace or arrows.

## Threat model

- **Cannot:** store what it types, use a network, send data to the computer, take commands from it, or be reflashed over USB (reflashing needs the BOOT button held while plugging in). Bluetooth firmware updates: bonded phone only, and refused by production firmware until images are signed.
- **Trust:** encrypted Bluetooth only; types only for a bonded phone. New phones pair only in a pairing window (first use, or 60 s after holding BOOT 3 s; BOOT 10 s erases all pairings). Outside it, bonding is off and unknown links are dropped; unauthenticated links drop after 30 s. LED blinks while the window is open.
- **Limits:** one phone connected at a time; messages up to 2,048 bytes from an 8 KB queue.
- **Residual risk:** pairing has no passkey ("Just Works"), so someone nearby during an open window could pair. A paired phone can type anything a keyboard can type into the focused window. Anyone holding the board can reflash it over USB, which serial-pinned rules contain.

## Windows: Group Policy

Only needed where device installation is restricted. Computer Configuration → Administrative Templates → System → Device Installation → Device Installation Restrictions:

1. **Allow installation of devices that match any of these device IDs**, both nodes:

```
USB\VID_2886&PID_0056
HID\VID_2886&PID_0056
```

2. **Apply layered order of evaluation for Allow and Prevent device installation policies across all device match criteria**, so the ID rule beats class-level Prevent rules (instance ID > device ID > setup class > removable).
3. Per unit: the device instance ID policy with `USB\VID_2886&PID_0056\<serial>` plus the keyboard node's instance ID (Device Manager or `pnputil /enum-devices /ids`).

## Windows: Intune (custom OMA-URI, String)

```
./Device/Vendor/MSFT/Policy/Config/DeviceInstallation/AllowInstallationOfMatchingDeviceIDs
<enabled/><data id="DeviceInstall_IDs_Allow_List"
value="1&#xF000;USB\VID_2886&amp;PID_0056&#xF000;2&#xF000;HID\VID_2886&amp;PID_0056"/>

./Device/Vendor/MSFT/Policy/Config/DeviceInstallation/EnableInstallationPolicyLayering
<enabled/><data id="AllowDenyLayered" value="1"/>
```

**Defender for Endpoint:** usually nothing to do. Its device control covers portable devices, removable media, CD/DVDs and printers (Windows) and removable media, Apple, portable and Bluetooth devices (macOS), not keyboards.

## CrowdStrike Falcon Device Control

USB classes are ANY, AUDIO_VIDEO, IMAGING, MASS_STORAGE, MOBILE, PRINTER, WIRELESS (no keyboard class). If Device Control activity shows it blocked, add a FULL_ACCESS exception in the reported class, for the user's host group:

```
Vendor ID 10374 · Product ID 86 · Serial <unit serial>
Combined ID: 10374_86_<serial>
```

## macOS

- Apple-silicon laptops ask "Do you want to connect the USB accessory to this Mac?": the user clicks Allow.
- MDM: `allowUSBRestrictedMode` = false (`com.apple.applicationaccess`, macOS 13+, supervised) skips the prompt for *every* new accessory, so letting the user approve the prompt is the narrower choice.
- Keyboard Setup Assistant may open: close it or pick ANSI. Jamf Protect device controls cover removable storage only.

**Citrix / VDI:** keep it on the local machine; do not redirect it.

Full details, the user's "ask before you plug it in" guide, a template email and vendor sources: the **For IT** page, https://dictationdongle.bronsonhill.com.au/it/. Steps were checked against Microsoft, CrowdStrike API, Apple and Jamf documentation on 21 November 2026; CrowdStrike's console docs need a login and were not checked. Not tested against your configuration: test on one machine first and read the IDs from a real unit.