

Spionážní technika

USB Keylogger AirDrive / Pro / Max

Návod k obsluze



Kontakt na dodavatele

SHX Trading s.r.o.

V Háji 15, Praha 7, 170 00

e-mail: podpora@spionazni-technika.cz

1. Vlastnosti výrobku

- Zaznamenává úhozy z jakékoliv USB klávesnice
- Nejmenší keylogger na trhu s délkou jen 21mm (verze MAX je o něco větší)
- Uloží až 8000 stránek textu
- 16MB interní flash paměť (verze MAX 8GB)
- 100% utajený, nezjistitelný bezpečnostním software
- Podporuje přes 40 různých rozložení klávesnic
- Kompatibilní se čtečkami čárových kódů
- Funguje jako Wi-Fi hotspot
- Připojení z jakéhokoliv počítače, smartphonu, nebo tabletu
- Přístup k datům z webového prohlížeče, bez speciálního softwaru nebo aplikace
- Získání dat vzdáleně, bez fyzického kontaktu se zařízením
- Jednoduché a srozumitelné WWW rozhraní
- Podporuje zabezpečení sítě WEP, WPA, a WPA-2
- Paměť chráněna hardwarovým šifrováním
- Verze PRO nabízí navíc Zasílání reportů e-mailem (viz kapitola 4),
- Zaznamenávání času (kapitola 5) a Živé streamování dat (kapitola 6).
- Verze MAX nabízí vše, co verze PRO a navíc jí lze použít jako Flash Disk s kapacitou 8GB.

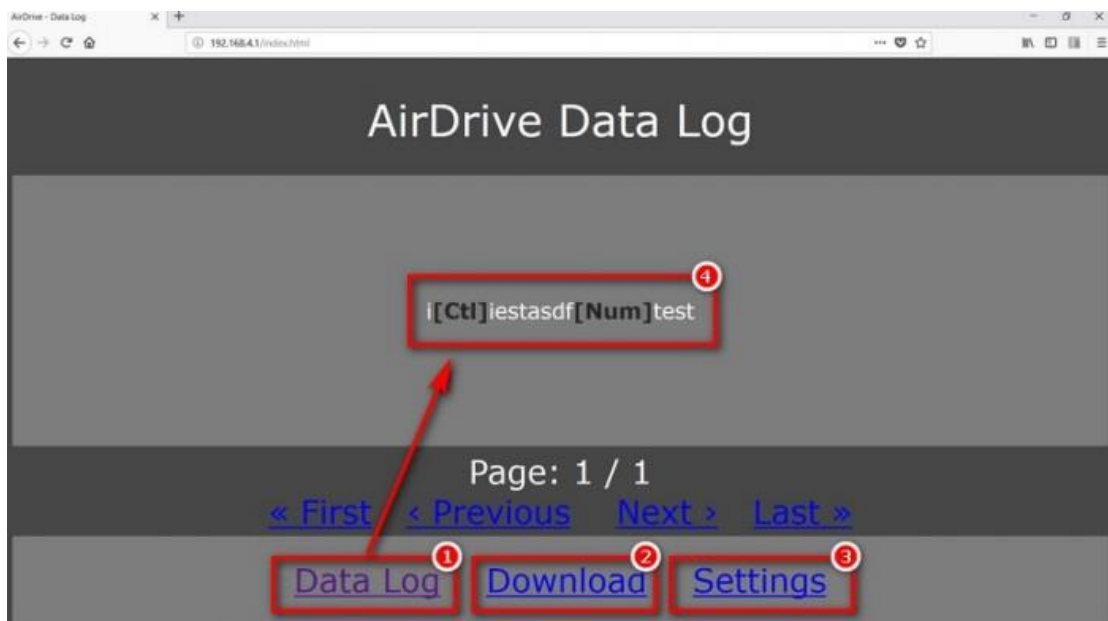
2. Rychlý start

Tato část obsahuje stručné pokyny pro základní ovládání keyloggeru. Pokud potřebujete podrobnější informace, věnujte pozornost dalším kapitolám.

1. Zapojte USB konektor od klávesnice do keyloggeru. Keylogger pak zapojte do USB vstupu na počítači (viz obr. níže).



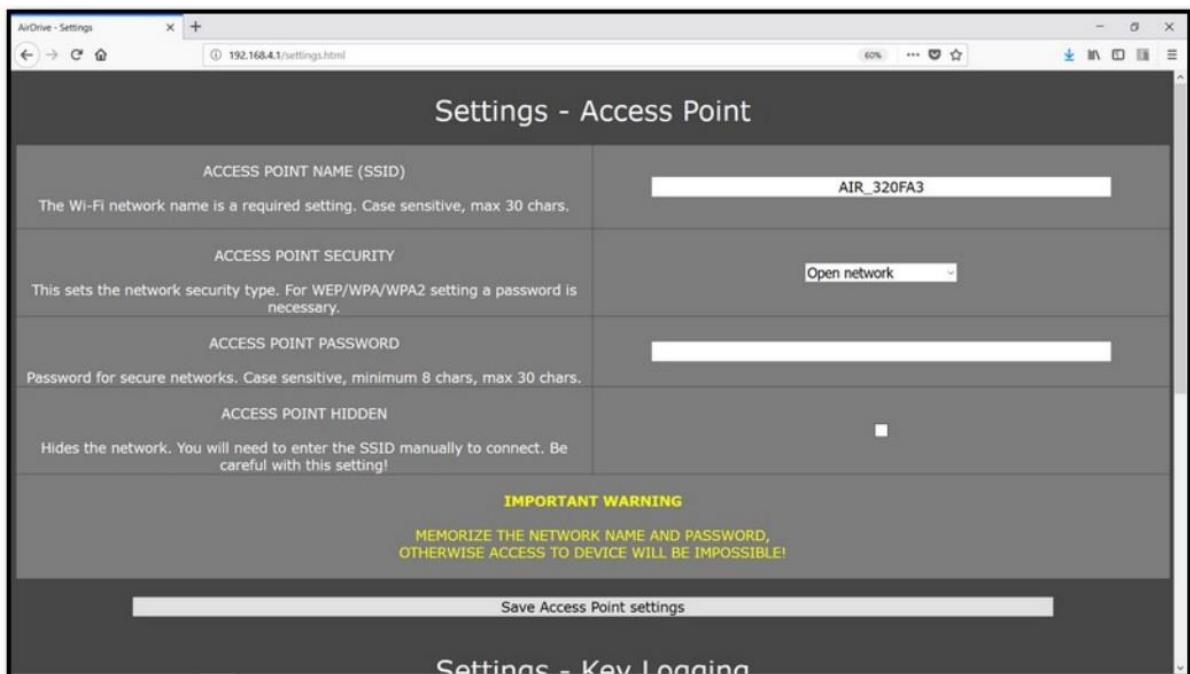
2. Použijte telefon, tablet, laptop, nebo počítač pro připojení k Wi-Fi síti keyloggeru. Název této sítě má tvar AIR_XXYYZZ (např. AIR_99D6D0).
3. Ve webovém prohlížeči otevřete adresu 192.168.4.1
4. Text zadaný na klávesnici si můžete (viz obrázek na další straně):
 - e. prohlédnout [4] kliknutím na volbu **Data Log** [1].
 - f. stáhnout jako textový soubor kliknutím na **Download** [2] a následně **Download Log File**.
5. Kliknutím na **Settings** [3] se dostanete do nabídky s nastavením (viz kapitola 3).



3. Základní nastavení

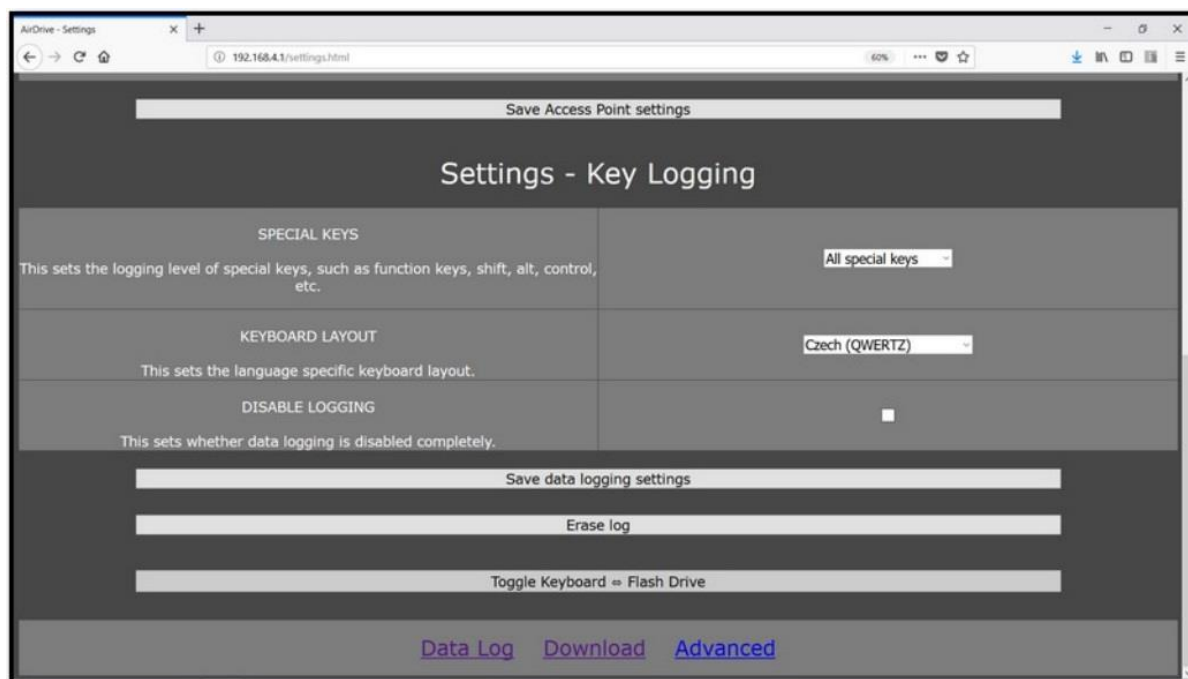
(Poznámka: ujistěte se, že si všechny přístupové údaje změněné v nastavení zapamatujete / zaznamenáte na bezpečném místě. V opačném případě ztratíte možnost se k zařízení připojit a používat ho.)

1. Po zapojení keyloggeru, připojení k jeho Wi-Fi síti a zadání IP adresy 192.168.4.1 ve webovém prohlížeči (viz kapitola **2. Rychlý start**), zvolte nabídku **Settings** (Nastavení).
2. V nastavení můžete měnit:
 - a. Nastavení přístupového bodu (**Settings – Access Point**):



- i. Název přístupového bodu (**Access Point Name (SSID)**),
Zde můžete zvolit libovolný název.
- ii. Druh zabezpečení (**Access Point Security**) a Vyberte druh zabezpečení, nebo volbou **Open Network** ponechte síť nezabezpečenou – bez nutnosti zadávat přihlašovací údaje.
- iii. Heslo přístupového bodu (**Access Point Password**).
Zde můžete nastavit přístupové heslo.

b. Nastavení zaznamenávání / logování (**Settings – Key Logging**):



i. Zaznamenávání speciálních znaků (**Special Keys**)

Zvolte, zda se mají zaznamenávat speciální znaky, jako Shift, Ctrl, Alt, NumLock, atd. Volba **All Special Keys** zaznamená všechny speciální znaky, volba **Some Special Keys** zaznamená hlavní speciální znaky, a volba **No Special Keys** zaznamená jen text. Aby byly zaznamenávány i číslice, zvolte volbu **All Special Keys**.

ii. Rozložení klávesnice (**Keyboard Layout**)

Zvolte rozložení odpovídající vaší klávesnici.

iii. Vypnutí zaznamenávání (**Disable Logging**)

c. Vymazání všech zaznamenaných údajů / logu (**Erase Log**)

d. Volba **Toggle Keyboard <=> Flash Drive** (dostupná jen u verze **MAX**)

Tato volba přepne zařízení z režimu *Keylogger/Keyboard* (zaznamenávání stisků kláves) na režim Flash disku. Postup je tedy takový, že necháme zařízení sledovat stisky kláves v režimu Keyboard a jen pokud chceme zařízení použít jako Flash disk (kapacita je 8GB), přepneme toto nastavení. Po přepnutí se zařízení v systému ohlásí jako USB Flash disk a můžeme ho použít na přenášení souborů, atp. Zároveň se na něm zobrazí soubor LOG.txt, ve kterém je zaznamenaná veškerá aktivita provedená na klávesnici do doby přepnutí této volby (v režimu **Flash Drive** se aktivita nezaznamenává!)

*Pozn.: k souboru LOG.txt se dostaneme i v režimu Keyboard, jak bylo popsáno v kapitole 2.4 (volba **Download > Download Log File**). Díky 8GB paměti poskytuje zařízení v podstatě neomezené úložiště pro zaznamenávání aktivity na klávesnici (pokud na něj nenahrajeme jiné objemné soubory).*

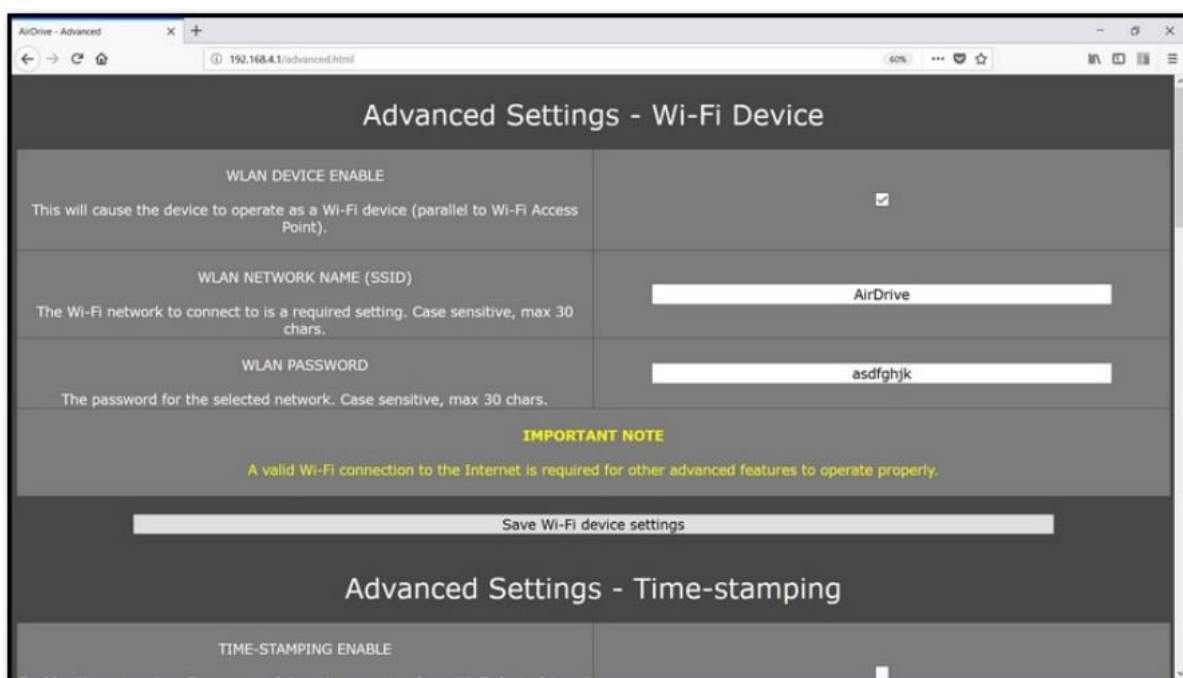
3. Změny uložte kliknutím na **Save Access Point settings** (Uložení nastavení přístupového bodu).

4. V případě, že jste změnili přihlašovací údaje, připojte se znovu k Wi-Fi síti keyloggeru za použití nových přihlašovacích údajů.

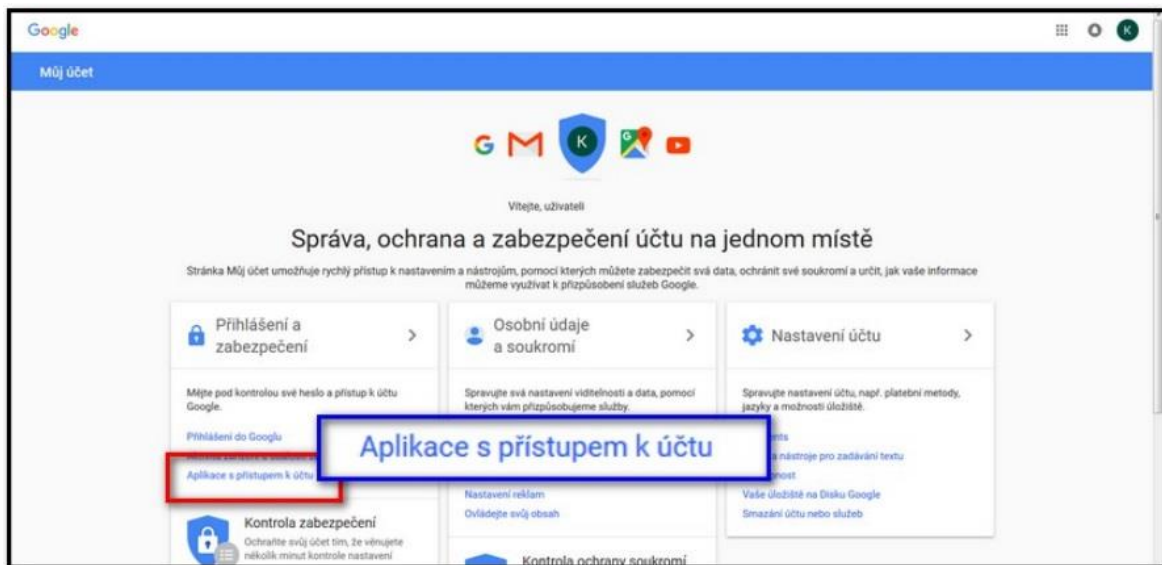
4. Zasílání reportů emailem (pouze verze Pro / Max)

(Poznámka: Pro zasílání e-mailů je potřeba keylogger připojit k internetu. Toho docílíme pomocí přístupového bodu s internetovým připojením, např. domácího routeru, viz **body 2-5**)

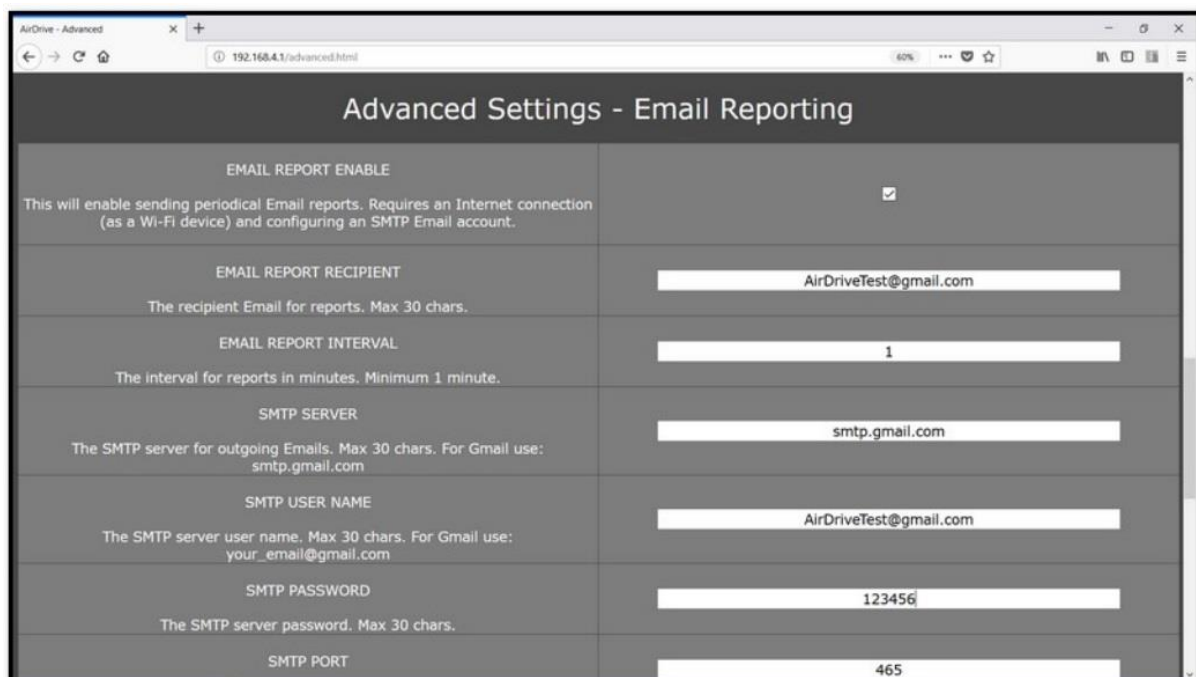
1. Připojte se k zařízení AirDrive (viz kapitola **Rychlý start**) a ve webovém prohlížeči otevřete adresu 192.168.4.1
2. V pokročilém nastavení (**Advanced Settings**) zaškrtněte volbu Používat zařízení v režimu Wi-Fi (**WLAN Device Enable**).



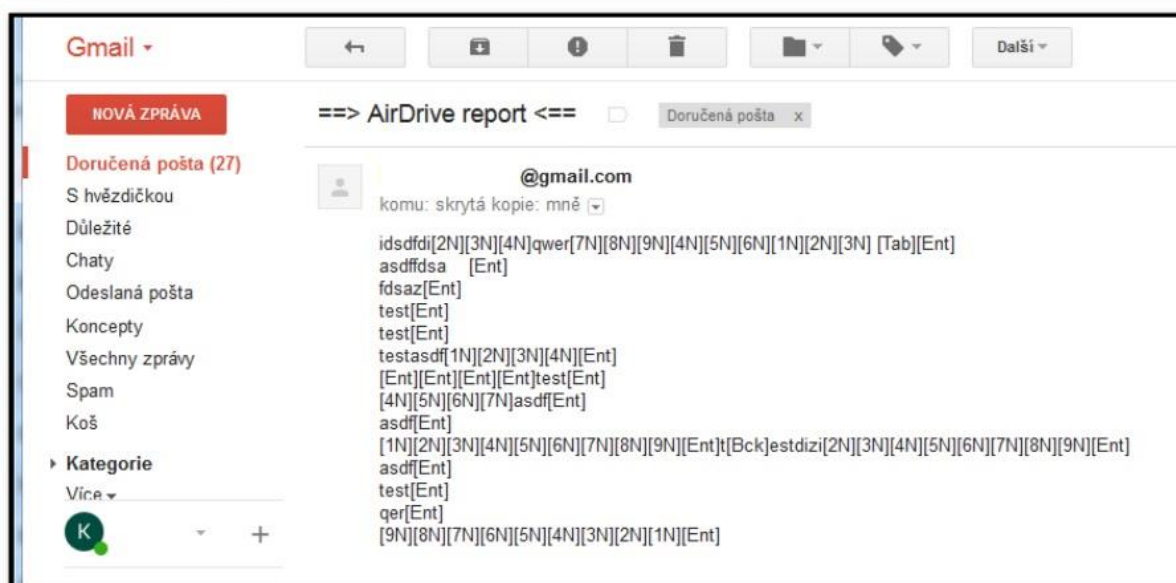
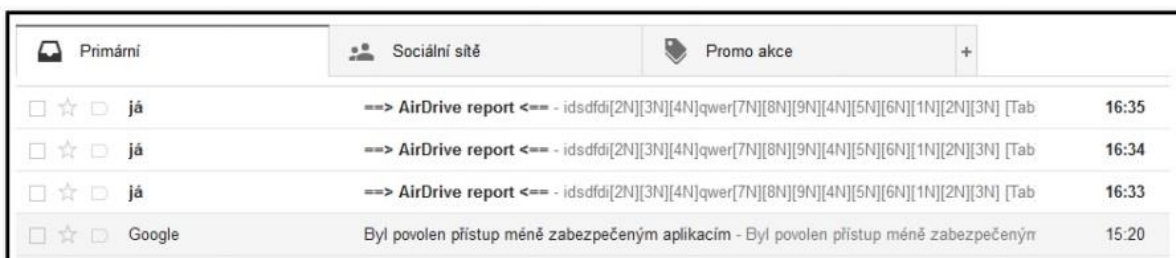
- U položky **WLAN Network Name (SSID)** zadejte název přístupového bodu, který chcete použít pro přístup k internetu.
- Zadejte heslo pro přístup do sítě zvoleného přístupového bodu pomocí volby **WLAN Password**.
- Uložte nastavení Wi-Fi (**Save Wi-Fi Device Settings**).
- AirDrive zasílá e-maily přes službu Gmail. Nejdříve je nutné změnit bezpečnostní nastavení účtu Google. Na stránce **myaccount.google.com** tedy po přihlášení v nastavení zvolte volbu **Aplikace s přístupem k účtu** (viz obr. níže).



- Povolte přístup méně bezpečným aplikacím (**Nastavení Povolit méně bezpečné aplikace: Zapnuto**).



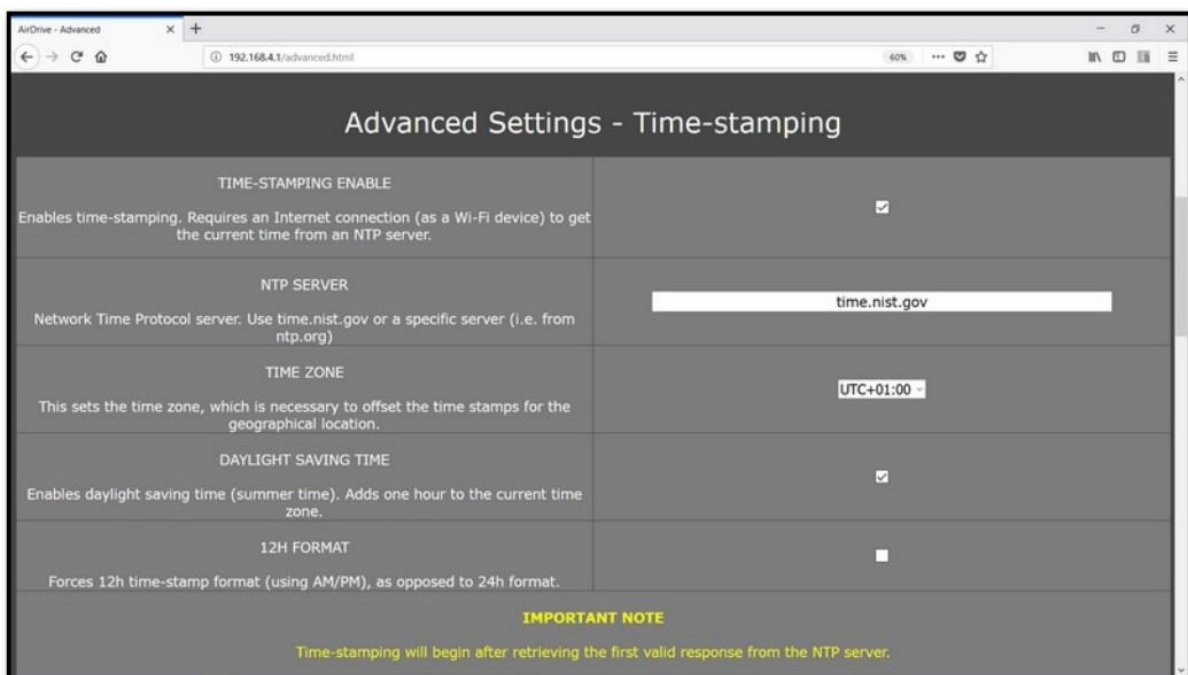
8. V pokročilém nastavení keyloggeru (192.168.4.1) zvolte sekci pro e-mailové reportování **Email Reporting** (viz obr. výše).
9. Povolte reportování zaškrtnutím volby **Email Report Enable**.
10. Do **Email Report Recipient** napište e-mailovou adresu, kterou chcete použít pro příjem reportů z keyloggeru. Můžete použít např. vaši Gmailovou adresu.
11. V **Email Report Interval** nastavte, jak často mají být reporty odesílány (minimum je 1 minuta).
12. Specifikujte server SMTP. Pro službu Gmail je to **smtp.gmail.com**.
13. **SMTP User Name** je v případě Gmailu vaše Gmailová adresa.
14. Zadejte své heslo do **SMTP Password** a číslo portu do **SMTP Port** (pro Gmail použijte hodnotu 465).
15. Uložte kliknutím na **Save Email Reporting Settings**.
16. Otevřete svou Gmail poštu a ujistěte se, že vám chodí reporty z vašeho AirDrive keyloggeru (viz obrázky níže).



5. Zaznamenávání data a času (pouze verze Pro / Max)

(Poznámka: Pro zaznamenávání času je potřeba keylogger připojit k internetu. Toho docílíme pomocí přístupového bodu s internetovým připojením, např. domácího routeru. - viz kapitola 4, body 2-5)

1. Připojte se k zařízení AirDrive (viz kapitola 2. **Rychlý start**) a ve webovém prohlížeči otevřete adresu 192.168.4.1
2. V pokročilém nastavení (**Advanced Settings**) v sekci **Time-stamping** zaškrtněte volbu Používat zaznamenávání času (**Time-Stamping Enable**).



3. Dále můžete v nastavení měnit:

a. **NTP Server**

Můžete zvolit server, který chcete použít pro získání času, nebo ponechat výchozí.

b. Časovou zónu (**Time Zone**)

V případě ČR je to UTC+01:00

c. Použití letního času (**Daylight Saving Time**)

d. 12 hodinový formát (**12H Format**)

- Uložte nastavení kliknutím na **Save Time-Stamping Settings**.
- Nyní zkontrolujte, zda jsou v logu (v prohlížeči i v textovém souboru) záznamy doplněné časovými údaji.

```

AirDrive Data Log

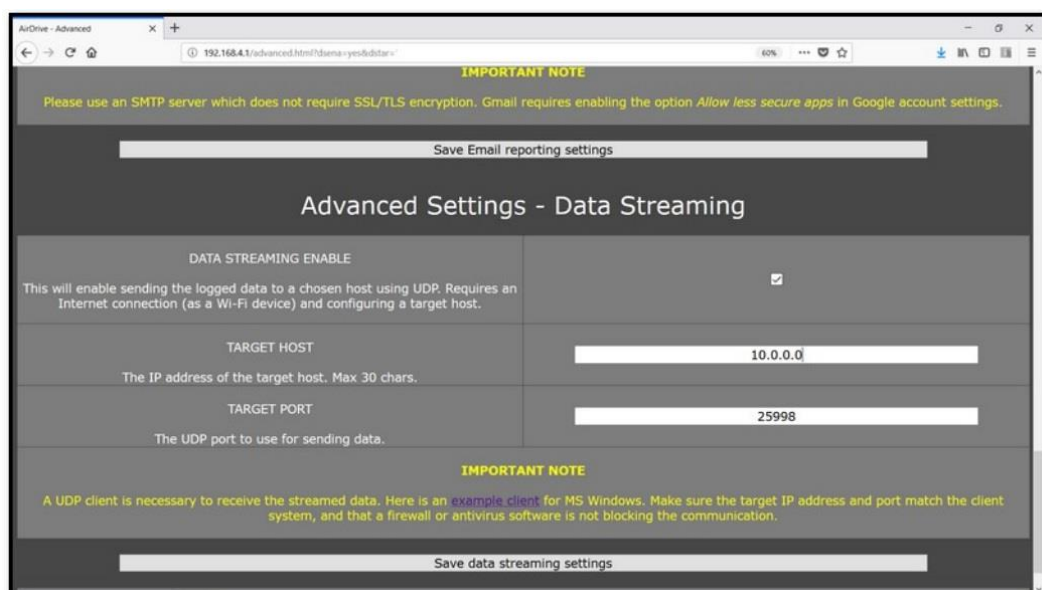
[2N][3N][4N]qwer[7N][8N][9N][4N][5N][6N][1N][2N][3N] [Tab]
asdfsda [Ent]
fdsaz [Ent]
test [Ent]
test [Ent]
testasdf [1N][2N][3N][4N][Ent]
[Ent][Ent][Ent][Ent]test [Ent]
[4N][5N][6N][7N]asdf [Ent]
asdf [Ent]
[5N][6N][7N][8N][9N][Ent]!Bck]estdizi [2N][3N][4N][5N][6N][7N]
asdf [Ent]
test [Ent]
qer [Ent]
[4N][3N][2N][1N][Ent]qqqd [2N][3N][4N][1N][2N][3N][4N][5N]
7777
[2018/3/8 18:45:43]time test [Ent]
[Ent]time test [Ent]
[Ent][Ent][Ent]

```

6. Živé streamování dat (pouze verze Pro / Max)

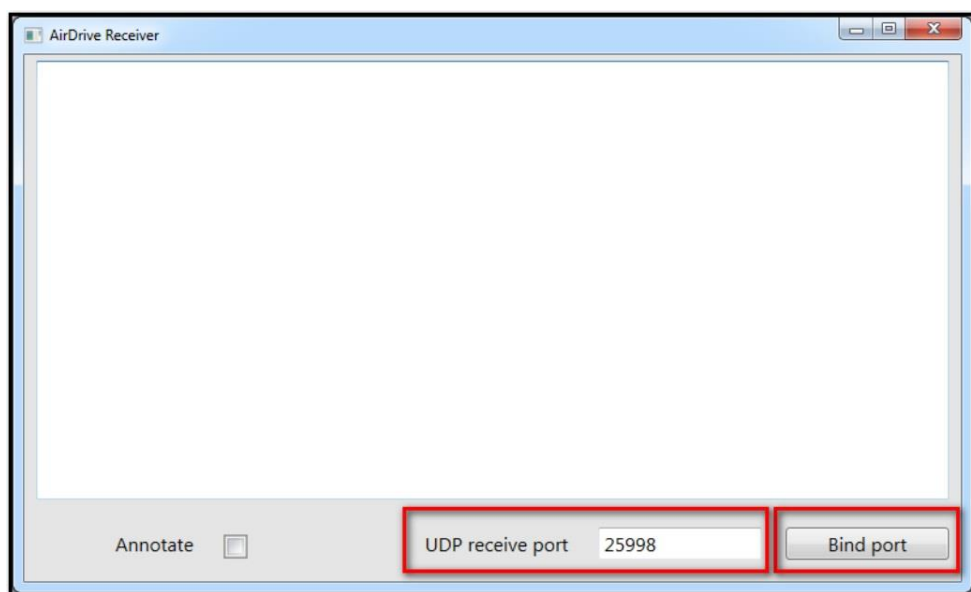
(Poznámka: Pro živé streamování je potřeba keylogger připojit k internetu. Toho docílíme pomocí přístupového bodu s internetovým připojením, např. domácího routeru. - viz kapitola 4, body 2-5)

- Připojte se k zařízení AirDrive (viz kapitola 2. **Rychlý start**) a ve webovém prohlížeči otevřete adresu 192.168.4.1
- V pokročilém nastavení (**Advanced Settings**) zaškrtněte volbu Používat zařízení v režimu Wi-Fi (**WLAN Device Enable**).
- U položky **WLAN Network Name (SSID)** zadejte název přístupového bodu, který chcete použít pro přístup k internetu.
- Zadejte heslo pro přístup do sítě zvoleného přístupového bodu pomocí volby **WLAN Password**.
- Uložte nastavení Wi-Fi (**Save Wi-Fi Device Settings**).

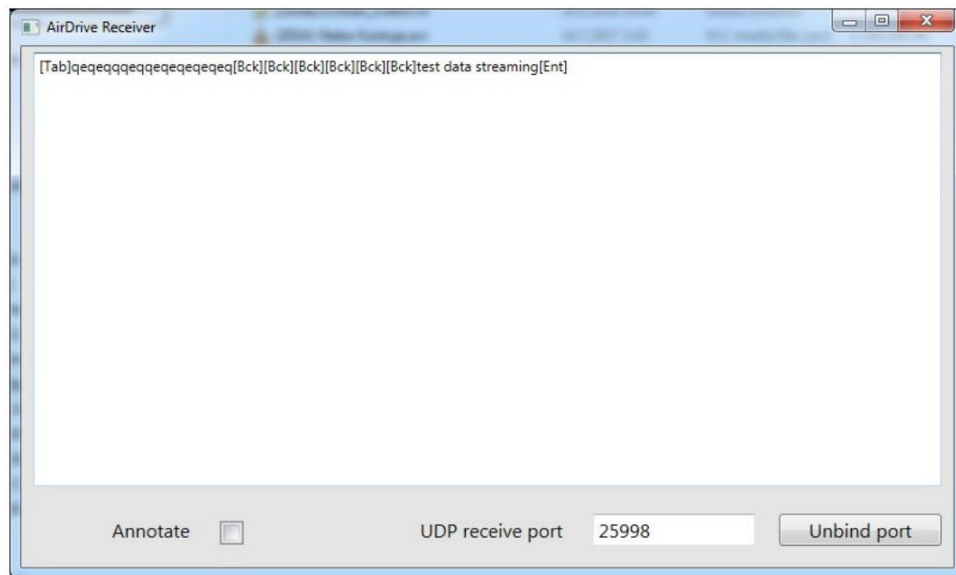


6. Nyní si zjistíte IP adresu cílového zařízení. Streamování dat lze uskutečnit pod téměř jakýmkoliv operačním systémem. V případě operačního systému Windows zjistíme IP adresu např. spuštěním programu cmd.exe (zadáním příkazu **cmd** v příkazovém řádku) a následným zadáním příkazu **ipconfig**.
7. Vraťte se do pokročilého nastavení (**Advanced Settings**) vašeho keyloggeru zadáním adresy 192.168.4.1 ve webovém prohlížeči. Zvolte nastavení **Data Streaming**. Zde povolte streamování dat zaškrtnutím **volby Data Streaming Enable** (viz obr. výše).
8. V části **Target Host** zadejte IP adresu cílového zařízení, kterou jste zjišťovali v bodu 6.
9. Vyplňte hodnotu pro cílový port (**Target Port**). Výchozí hodnota je 25998, ale lze použít jakoukoliv jinou hodnotu.
10. Uložte nastavení kliknutím na tlačítko **Save Data Streaming Settings**.
11. Nyní je potřeba se ujistit, že na zařízení, kde chcete streamování sledovat, je přítomna tzv. UDP aplikace.
 - a. Např. v OS Android si přes Google Play můžete takovou aplikaci vyhledat zadáním „UDP receiver“, nebo „UDP terminal“ a následně jí nainstalovat.
 - b. V OS Windows můžete použít UDP aplikaci, která je součástí vašeho AirDrive keyloggeru. Tu najdete v sekci nastavení (**Settings**). Kliknutím na odkaz **example client** si jí můžete stáhnout (je to soubor Receiver.exe).

*(Poznámka: V případě použití dodané aplikace se ujistěte, že firewall ani anti-virový program neblokuje komunikaci. Také se po spuštění programu ujistěte, že hodnota v políčku **UDP Receive Port** je totožná s hodnotou, kterou jste zadávali v bodu 9. Nakonec musíte kliknout na tlačítko **Bind Port**, aby došlo k úspěšné komunikaci přes vámi zvolený port – viz obr. níže.)*



c. Pokud je vše nastaveno správně, UDP klient bude v reálném čase zobrazovat vše, co se zadává na sledované klávesnici.



7. FAQ

Keylogger nebude fungovat s následujícími přístroji:

- Klávesnice notebooku
- Bluetooth klávesnice
- USB-PS2 a PS2-USB redukce

Klávesnice nereaguje:

- USB konektor nebo keylogger nejsou správně zastrčeny, zkontrolujte je
- Keylogger je aktivován pro čtení dat – v nastavení keylogger přepněte do režimu Keyboard viz kapitola 3.2.d
- Keylogger se nedaří přepnout do Flash Disk módu
- Zkontrolujte, zdali je keylogger zapojen dle tohoto návodu, viz kapitola 3.2.d

Nefunkčnost národních charakteristik v reportech

- Zkontrolujte, zdali je v nastavení zvoleno správné rozložení klávesnice, viz kapitola 3.2.b.ii.

Všechno jsem již prověřil, nic nepomohlo!

Pokud trable přetrvávají, postupujte následovně:

1. Prověřte, že problémy přetrvávají i na jiné klávesnici
2. Pokud je to možné, prověřte, že problémy přetrvávají i na jiném PC
3. Obratě se na nás na našich kontaktech

8. Specifikace

Napájení	4,5 – 5,5V DC (čerpáno z USB portu)
Spotřeba	65mA (0,33W)
Podpora klávesnice	USB-HID kompatibilní (Low / Full / High-speed)
Max. ukládací rychlost (špičk.)	přibližně 500 bytů/s
Běžná ukládací rychlost	cca 100 bytů/s
Kapacita paměti	16MB – 8GB
Výdrž dat	100 let
Max. rychlost zobrazení	150 kB/s
Rozměry vč. konektoru	35 mm x 20 mm x 12 mm (verze MAX 55 mm x 18 mm x 8 mm)



9. Závěrečná ustanovení

Ovládání přístroje se může v závislosti na jednotlivých sériích drobně lišit.

Přístroj používejte v souladu s platnými právními předpisy. Dodavatel nenesе žádnou odpovědnost za použití přístroje v rozporu s těmito předpisy.

Návod je majetkem společnosti SHX Trading s.r.o. Veškeré kopírování, či jiné používání musí být se souhlasem této společnosti.

Pokud v návodu naleznete nějaké nepřesnosti, budeme rádi, pokud nás budete informovat na našem e-mailu: podpora@spionazni-technika.cz