

Yubikey beállítása a GreenRADIUS-hoz (OTP módban)

1. BEVEZETŐ

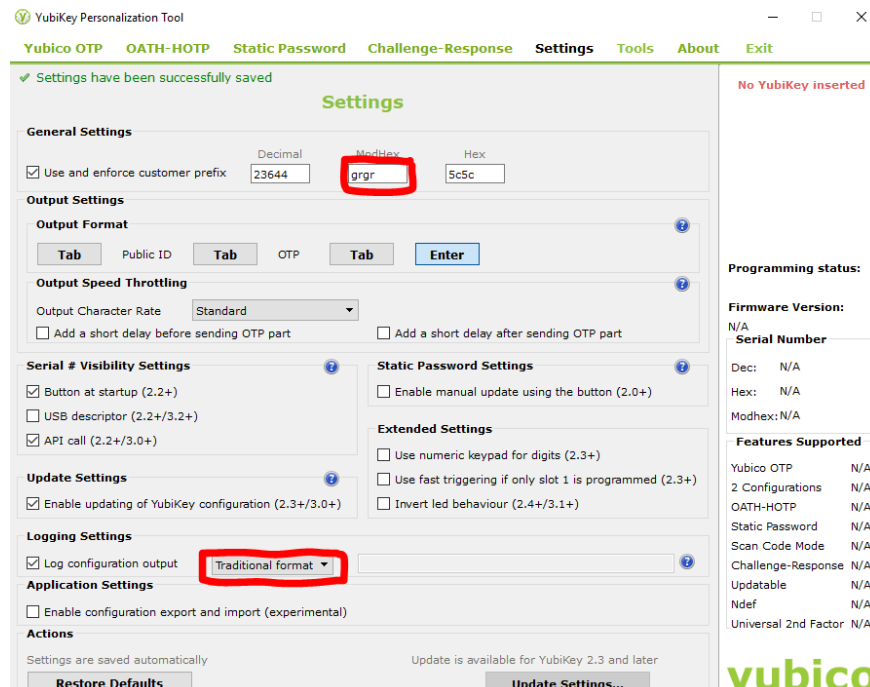
Ez a leírás bemutatja, hogyan állítsuk be a Yubikey kulcsokat OTP módban, hogy a titkosításnál használt információk - továbbiakban secrets - a helyben futó GreenRADIUS kiszolgálón kerüljenek eltárolásra, a Yubikey alapbeállításai helyett, mely a YubiCloudban tárolná ezeket az adatokat.

2. ELŐFELTÉTELEK

- Legyen nálunk az összes Yubikey amit fel akarunk programozni
- Töltsük le és telepítsük fel a Yubico Personalization Tool-t a gépünkre (innen)

3. YUBIKEY KULCSOK FELPROGRAMOZÁSA

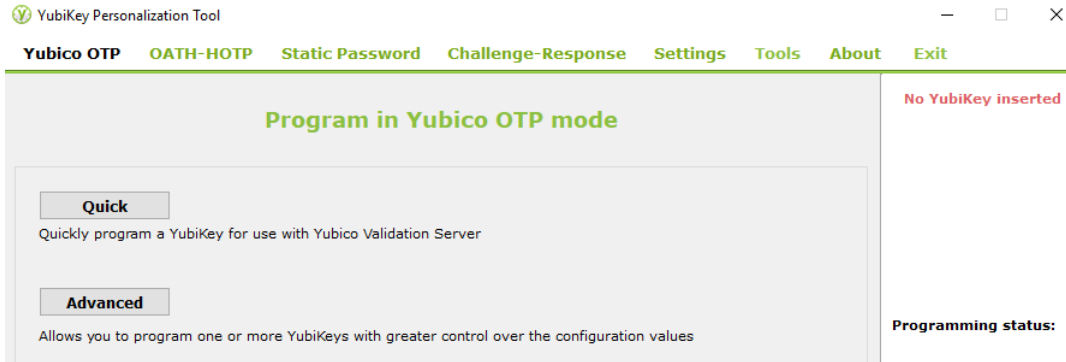
1. Nyissuk meg a Yubico Personalization Tool-t
2. Válasszuk ki a "Settings" menüpontot
 - a. Kattintsuk be "Use and enforce customer prefix"-t és a ModHex mezőbe írjuk be, hogy "grgr"
 - b. Válasszuk ki a "Traditional format" a "Log configuration output" részben



The screenshot shows the Yubico Personalization Tool interface. The 'Settings' tab is active. In the 'General Settings' section, the 'Use and enforce customer prefix' checkbox is checked, and the 'ModHex' field contains 'grgr'. In the 'Logging Settings' section, the 'Log configuration output' checkbox is checked, and the dropdown menu is set to 'Traditional format'. The 'Update Settings' section has 'Enable updating of YubiKey configuration' checked. The 'Application Settings' section has 'Enable configuration export and import' unchecked. The 'Actions' section shows 'Settings are saved automatically' and 'Update is available for YubiKey 2.3 and later'. The 'Restore Defaults' and 'Update Settings...' buttons are visible at the bottom. On the right side, there is a 'Programming status' section showing 'No YubiKey inserted' and a 'Features Supported' table.

| Feature | Status |
|----------------------|--------|
| Yubico OTP | N/A |
| 2 Configurations | N/A |
| OATH-HOTP | N/A |
| Static Password | N/A |
| Scan Code Mode | N/A |
| Challenge-Response | N/A |
| Updateable | N/A |
| Ndef | N/A |
| Universal 2nd Factor | N/A |

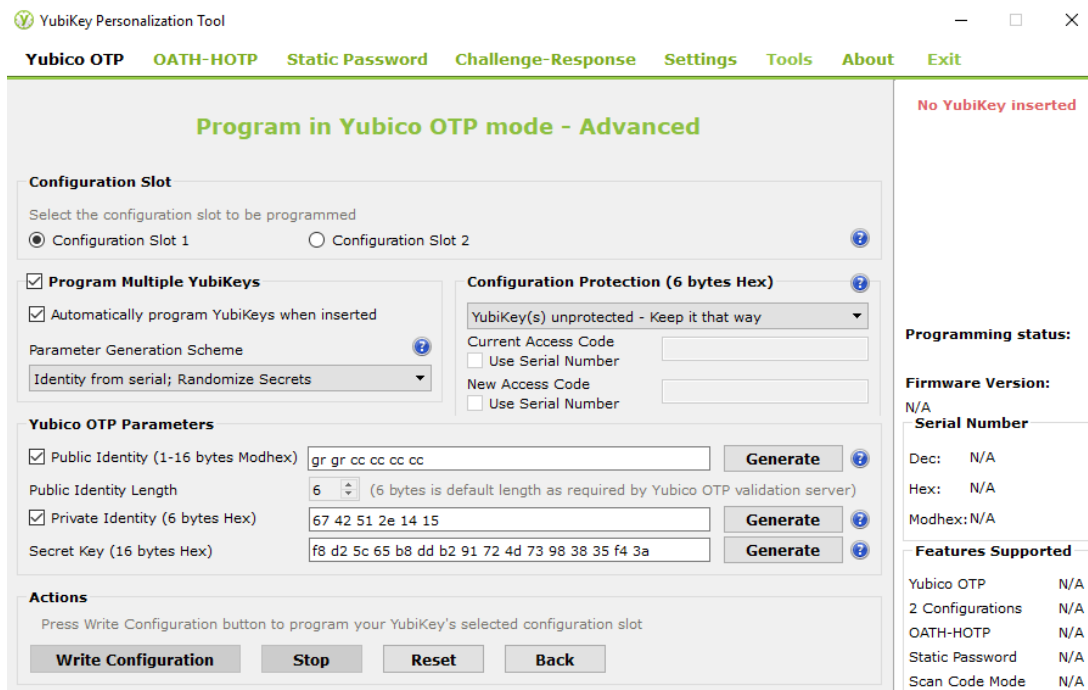
3. Válasszuk ki a "Yubico OTP" menüpontot és kattintsunk az "Advanced" gombra



The screenshot shows the 'YubiKey Personalization Tool' window. The 'Yubico OTP' menu item is selected. The main area displays 'Program in Yubico OTP mode' with two buttons: 'Quick' and 'Advanced'. The 'Advanced' button is highlighted. The right sidebar shows 'No YubiKey inserted' and 'Programming status:'.

4. A következő képet fogjuk látni lásd alább:

- Válasszuk ki a "Configuration Slot 1"-t
- Válasszuk ki a "Program Multiple Yubikeys"-t
- Válasszuk ki a "Select Automatically program YubiKeys when inserted"-t
- Az "Under Parameter Generation Scheme" alatt válasszuk a "Identity from serial; Randomize Secrets" opciót



The screenshot shows the 'YubiKey Personalization Tool' window in 'Advanced' mode. The 'Configuration Slot' section has 'Configuration Slot 1' selected. The 'Program Multiple YubiKeys' checkbox is checked, along with 'Automatically program YubiKeys when inserted'. The 'Parameter Generation Scheme' is set to 'Identity from serial; Randomize Secrets'. The 'Yubico OTP Parameters' section shows 'Public Identity' (gr gr cc cc cc cc), 'Private Identity' (67 42 51 2e 14 15), and 'Secret Key' (f8 d2 5c 65 b8 dd b2 91 72 4d 73 98 38 35 f4 3a). The 'Actions' section includes 'Write Configuration', 'Stop', 'Reset', and 'Back' buttons. The right sidebar shows 'No YubiKey inserted', 'Programming status:', 'Firmware Version: N/A', 'Serial Number' (Dec: N/A, Hex: N/A, Modhex: N/A), and 'Features Supported' (Yubico OTP: N/A, 2 Configurations: N/A, OATH-HOTP: N/A, Static Password: N/A, Scan Code Mode: N/A).

5. Helyezzük be az első Yubikey és kattintsunk a "Write Configuration" gombra. Nevezzük el a kimeneti fájlt és mentjük el. (Megjegyzés: biztosítsuk, hogy a kimeneti fájl NE tartalmazzon szóköz karaktereket.) Ez a fájl fogja tartalmazni a felprogramozott Yubikey kulcsok biztonsági adatait. Kérjük tartsa biztonságos helyen addig amíg nem töltjük be a GreenRADIUS-ba.
6. A már behelyezett Yubikey felprogramozásra kerül és ebben az esetben annak sikerességéről szóló üzenetet kapunk. Távolítsuk el a Yubikey-t.
7. Anélkül, hogy kilépnénk az alkalmazásból, helyezzük be a következő Yubikey-t. Várjuk meg, hogy a program a behelyezett Yubikey-t felprogramozza (a sikerességről üzenetet kapunk), majd távolítsuk el. Folytassuk ezt a folyamatot a maradék Yubikey kulccsal.
8. Miután minden Yubikey-t felprogramoztunk, kattintsunk a "Stop" gombra és csukjuk be az alkalmazást.

4. AZ ÚJ SECRETS FÁJL IMPORTÁLÁSA A GREENRADIUSBA

1. Nyissunk meg egy új ablakot a böngészőben és menjünk a GreenRADIUS webes admin oldalra.
2. Győződjünk meg arról, hogy az ellenőrzést végző szerver "Local Validation Server on GreenRADIUS"-re legyen beállítva.

Module Index

Validation Server Configuration



Validation Server Configuration

Validation Server

YubiCloud - Online Validation Service

Local validation Server on GreenRADIUS Virtual Appliance

Other (for example: "http://192.168.1.1/wsapi/2.0/verify")

Save

[Return to Global Configuration](#)

3. Válasszuk ki az "Import Secrets" menüpontot.
4. Válasszuk ki a "Cross-Platform Personalization tool-Import YubiKey Secrets"-t és kattintsunk a "Browse..." gombra.

Module Config

GreenRADIUS - Virtual Appliance



Domain Global Configuration Diagnostics Troubleshoot Reports Updates **Import Secrets** List Tokens License Alerts About

Import Secrets

This section can be used to import the AES secrets in to the local YK-KSM or YubiHSM database if the local validation server on GreenRADIUS Virtual Appliance is used to validate the OTPs.

Log file source

Original Windows Personalization tool-Import YubiKey Secrets

Cross-Platform Personalization tool-Import YubiKey Secrets

Import OATH Tokens (PSKC Container)

Select a file to upload No file selected.

Upload

5. Válasszuk ki a felprogramozáskor létrehozott fájlt.
6. Kattintsunk az "Upload" gombra. Ne menjünk el a weboldalról. Várjuk meg a sikerességet megjelenítő üzenetet.
7. Miután a feltöltés sikerült, az újonnan importált tokeneket a "List Tokens" fül alatt láthatjuk.