

Wanneer het niet mogelijk of wenselijk is om via een Mobiele telefoon of Tablet gebruik te maken van de Google Authenticator App, kan er gebruik gemaakt worden van een Windows Applicatie om de code te genereren.

Hoewel Google zelf geen applicatie levert, zijn er wel applicaties beschikbaar die door andere partijen zijn ontwikkeld.

Een voorbeeld hiervan is *WinAuth*. Dit is een opensource applicatie waarmee op een Windows Desktop de Google code kan worden gegenereerd op basis van de 'Geheime Sleutel'.

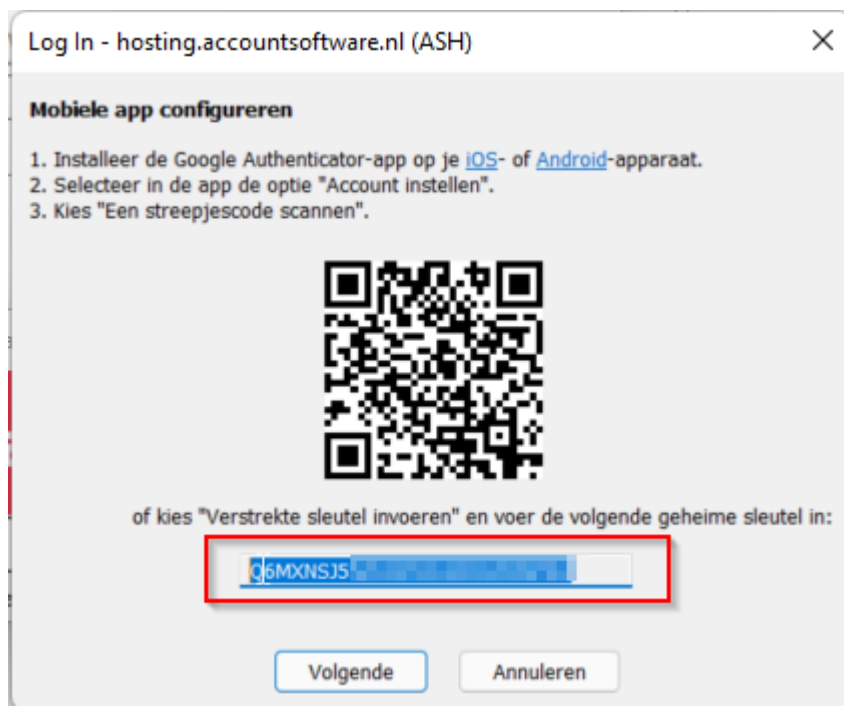
*WinAuth* is verkrijgbaar via <https://winauth.github.io/winauth/download.html>

Via onze website is een installer beschikbaar die deze applicatie in het lokale gebruikersprofiel installeert en een snelkoppeling op het bureaublad aanmaakt.

[https://download.accountsoftware.nl/WinAuth\\_installer.exe](https://download.accountsoftware.nl/WinAuth_installer.exe)

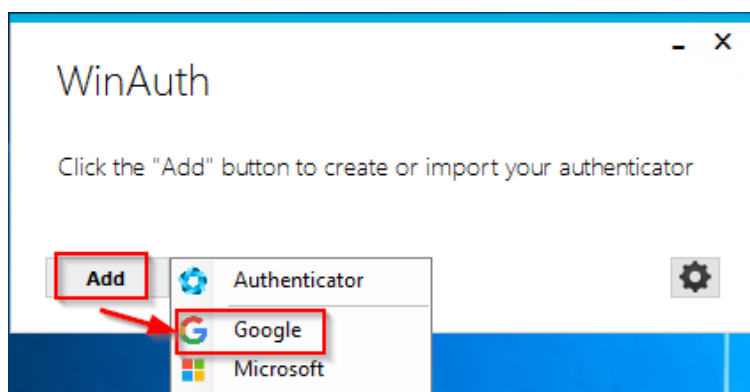
Wanneer MFA in de hosting geactiveerd moet worden, toont het inlogscherf de eerste keer een code (de geheime sleutel) en een QR-code.

Deze code is nodig om het account in WinAuth te koppelen.



Kopieer de geheime sleutel uit het inlogscherf.

Installeer WinAuth en start de applicatie:



Klik op **Add** en vervolgens op **Google**

**Add Google Authenticator**

Name:

Icon:

1. Enter the Secret Code for your authenticator. Spaces don't matter. If you have a QR code, you can paste the URL of the image instead.

2. Click **Verify Authenticator**

3. Verify the following code matches your service

**OK** **Cancel**

Tip: Vul bij **Name** ook de naam in van het hostingaccount waar de code voor is. Vul de geheime sleutel in in het veld en klik op **Verify Authenticator** en **OK**.

**Protection**

Select how you would like to protect your authenticators. Using a password is strongly recommended, otherwise your data could be read and stolen by malware running on your computer.

**Protect with my own password**

Your authenticators will be encrypted using your own password and you will need to enter your password to open WinAuth. Your authenticators will be inaccessible if you forget your password and you do not have a backup.

Password

Verify

Additionally, you can protect and encrypt your data using the built-in Windows account encryption. This will lock your authenticators to this computer or user so they cannot be opened even if the files are copied. You **MUST** turn this off if you are going to reformat your disk, re-install Windows or delete this user account.

Encrypt to only be useable on this computer

And only by the current user on this computer

Lock with a YubiKey

Your YubiKey must support Challenge-Response using HMAC-SHA1 in one of its slots. Use the YubiKey personalization tool to configure the slot or click the Configure Slot button.

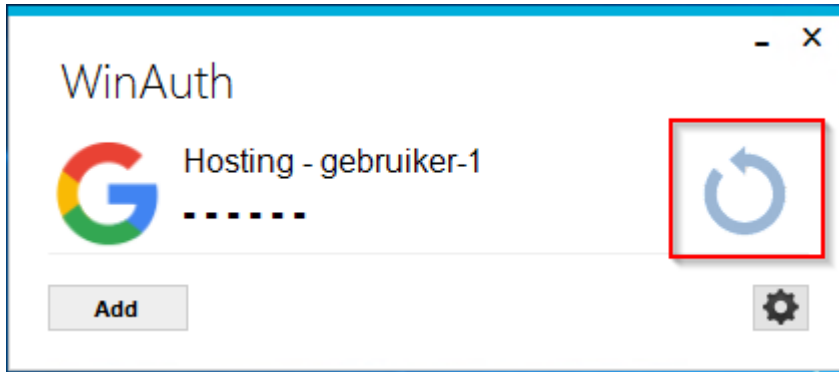
Slot 1

**Use Slot** **Configure Slot**

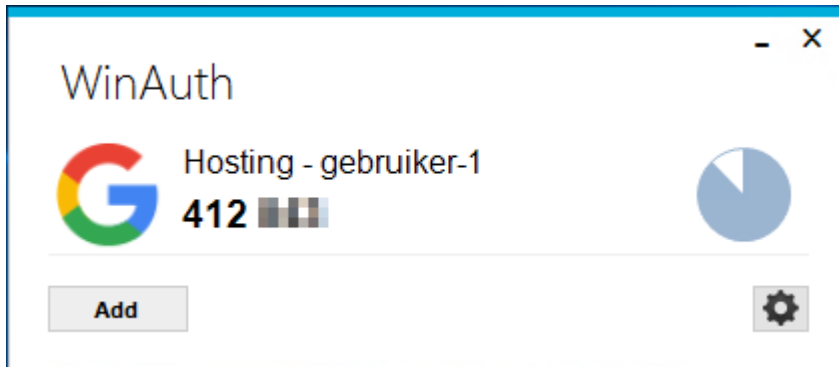
**OK** **Cancel**

Kies tot slot of er voor het tonen van de code om een extra wachtwoord gevraagd moet worden. Klik daarna op **OK**.

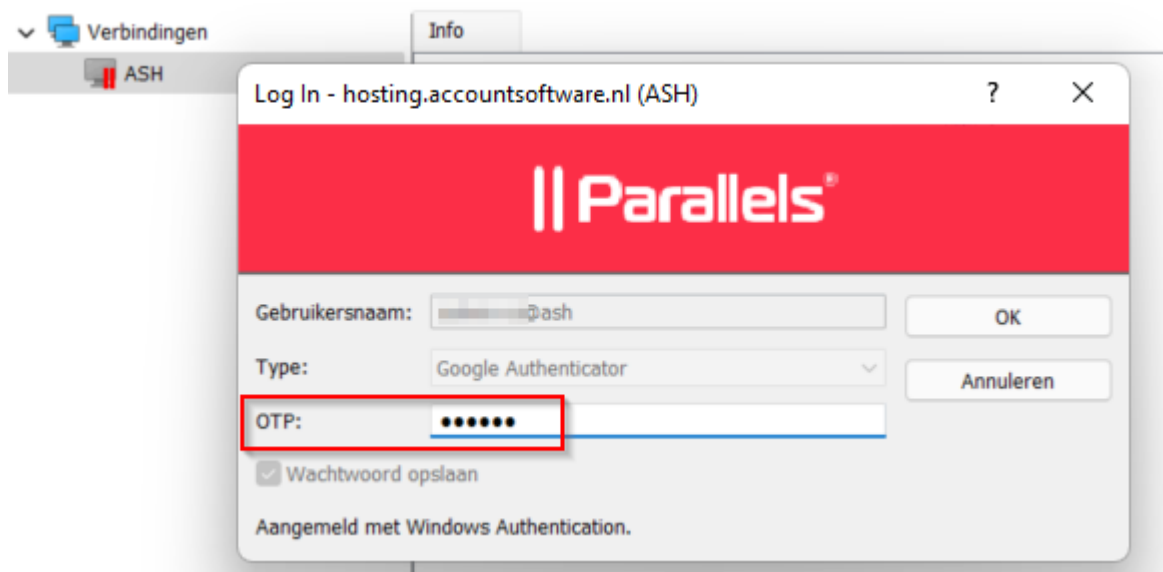
Nu is de configuratie opgeslagen en zal de applicatie na het starten de codes kunnen laten zien:



Klik op het **ververs-icoontje** om een code te laten zien



Deze code kan vervolgens ingevoerd worden in het inlog dialoog van Parallels.



*Let op:*

*Het gebruik van deze applicatie is voor eigen risico. Het is een Open-source applicatie. We kunnen geen support hierop geven of verantwoordelijkheid nemen voor gevolgen van het gebruik van deze applicatie.*