

Authenticating to HamWAN services with an authenticator

Introduction

HamWAN is an amateur radio network which provides access to a variety of services. Some of these services require you to be authenticated (verify who you are). Because HamWAN is primarily an amateur-radio based network, encryption is not permitted. A lack of encryption makes traditional password-based authentication insecure, as an attacker can easily capture a user's credentials and impersonate them.

To overcome these challenges HamWAN Victoria has implemented a custom authentication mechanism based on the TOTP protocol. TOTP involves two components: the server-side verification and a client-side authenticator. The client authenticator is something that you (the user) possess and is an application that either runs on a PC or a Smartphone.

Recommended authenticators are:

- 1) Google Authenticator (<https://support.google.com/accounts/answer/1066447?hl=en>) for iOS or Android phones
- 2) WinAuth (<https://www.winauth.com>) for PCs.

***Other TOTP authenticators may be compatible and while you are free to use them they are not supported.**

In this guide we will be showing you how to authenticate using WinAuth, but other authenticator clients will be similar.

Getting Started

First off, install your authenticator on either your PC or Smartphone. Next, navigate to <https://generate.vidigital.ca> – note that you MUST access this website from OUTSIDE of HamWAN as it needs to be an encrypted site as you will be retrieving sensitive data from it. Once the initial configuration of your authenticator has been completed, no sensitive data will be sent between your PC and the server, so you may reconnect to HamWAN. You must also specifically request an account by reaching out to us at <http://vidigital.ca/contact>. Once we have received your request we will prepare your account which will enable you to proceed with next steps.

You cannot continue until you have received confirmation from VI Digital that your account has been created.

Generate your secret code

- 1) Once you have received your confirmation, ensure you are connected to the Internet from a connection external to HamWAN (such as your home Internet, coffee shop, etc) and then browse to <https://generate.vidigital.ca>.
- 2) Scroll down to the bottom of the page and enter your callsign and press 'Get Started'

Registered a callsign? Get started!

If you have already registered your callsign (and received your confirmation email), enter it in the form below to get started!

Callsign:

Figure 1 – Registering your callsign

- 3) The website will process your request and should return a success message similar to the one below:

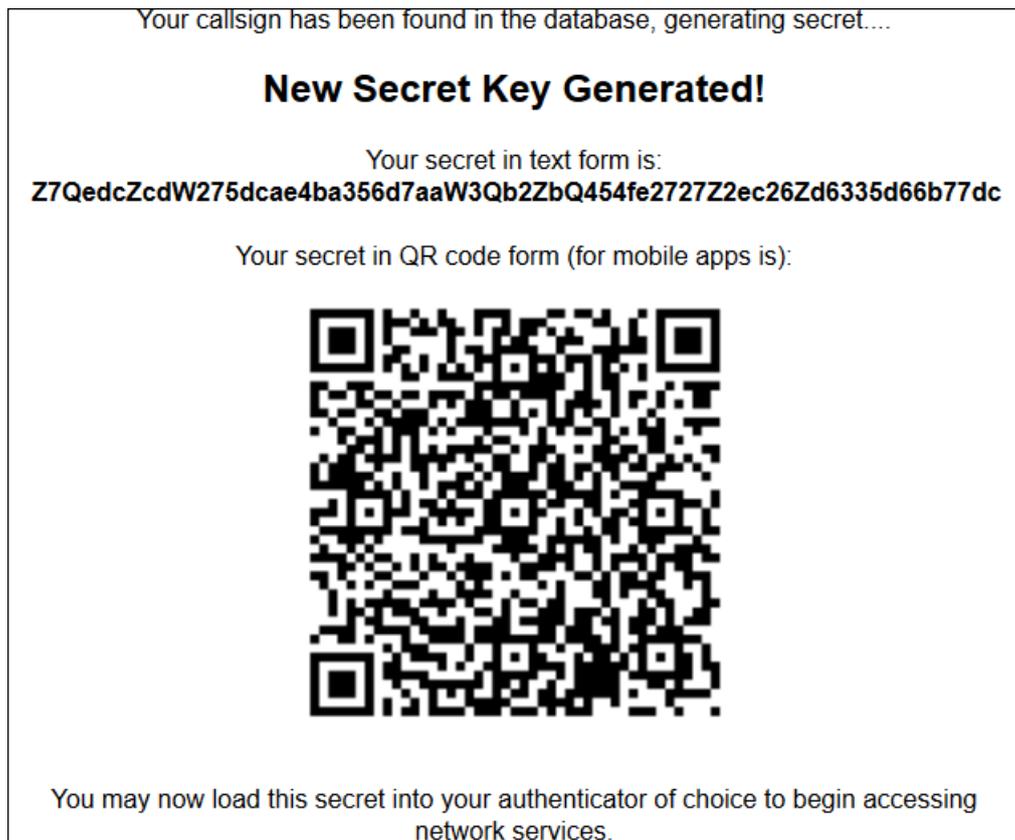


Figure 2 – Generated secret key

- 4) Now Open the WinAuth executable (or whichever program you have chosen as an authenticator). If using WinAuth click the option to 'add' and select 'authenticator' from the drop down menu.

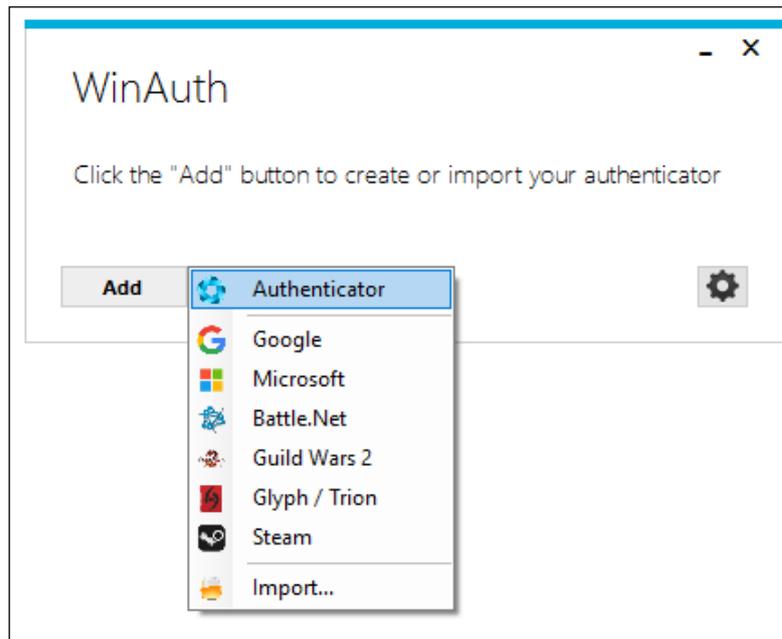


Figure 3 – Adding a new authenticator

- 5) In the next screen you will need to assign a descriptive name to your authenticator as well as input the secure secret you obtained in step 3. To reduce the possibility of error COPY and PASTE the key into WinAuth. Click 'verify authenticator' to generate a test code.

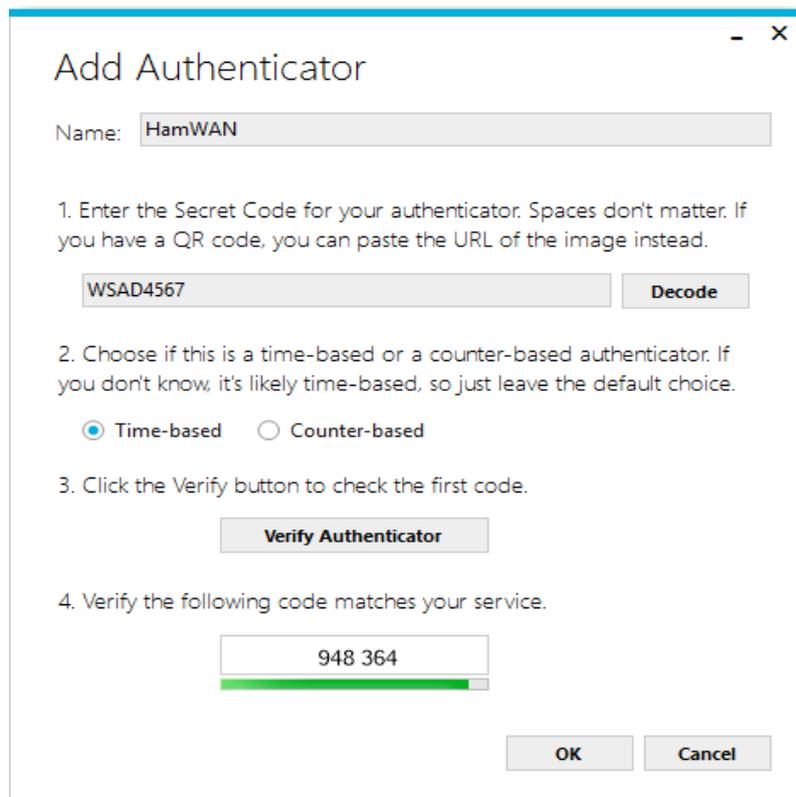


Figure 4 – Inputting details to WinAuth

- 6) Test the code by inputting it into <http://auth.vidigital.ca> along with your callsign

Login to VI Digital

Please use your client side authenticator to generate a code to login. Codes are valid for 30 seocnds after being generated.

Username/Callsign:

Authenticator Code:

Figure 5 – Testing credentials

- 7) You should be greeted with a success message. If you receive an error, double check the secret key you put into WinAuth
- 8) Once you have verified that WinAuth is generating valid codes you will need to save the authenticator. Press 'OK' on the test page.
- 9) You should then be presented with an option to set a password to secure your authenticator. While a password is not mandatory (i.e. it can be unselected), it is advisable if multiple people are accessing the computer

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

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

Figure 6 – Saving your authenticator

10) Press 'OK' and you should be returned to the main WinAuth Screen.

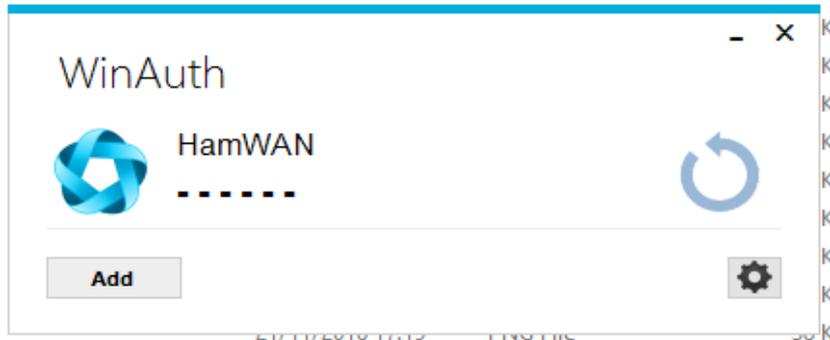


Figure 7 – New Authenticator

11) To View the current authentication code, press the large refresh button to the right of the WinAuth window

12) Once the text is visible, you can copy the code by right clicking/ You may then paste the code to the application you are logging into

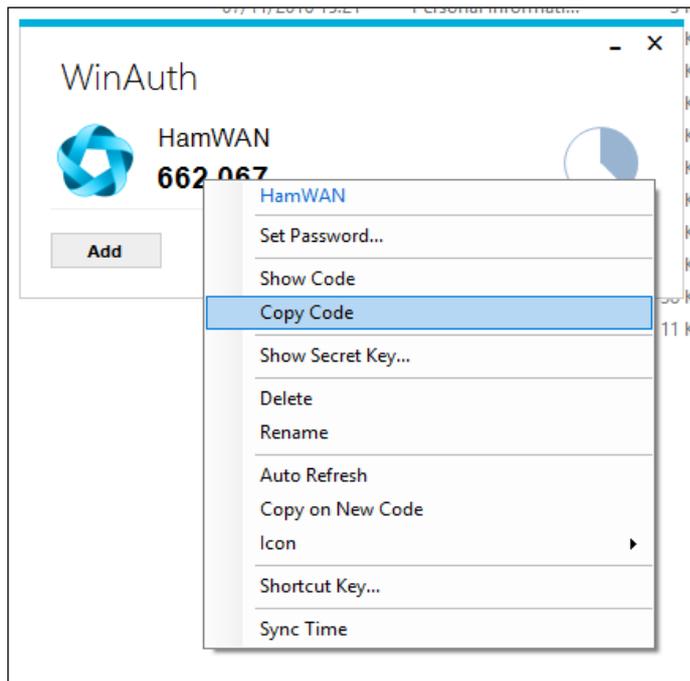


Figure 8 – Copying from WinAuth

Congratulations! You are now able to login to HamWAN services. At this point no sensitive data needs to be exchanged between the server and your computer so you may connect to HamWAN if applicable.

Note, that if you need to retrieve your authentication code at a later date (for instance if you wanted to add a new authenticator client), you can login at <http://auth.vidigital.ca> and follow the links.

Please complete this step OFF the HamWAN network (i.e. from a commercial Internet connection) as it requires encryption.