# Multi-Factor-Authentication for Zadara Storage

## Overview

Protecting access to systems by passwords is not considered secured enough. Sometimes, passwords are compromised or stolen or phished out. Nowadays, cybercriminals have automated tools that can make millions of guesses, and break into your account even if a strong password was used. Two Factor Authentication (often abbreviated as 2FA) is a mechanism that gives another layer of protection in case something like this happens.

All Zadara's Web applications: VPSA GUI, Command Center and Provisioning Portal provide an additional layer of security to its base username/password authentication. Two-Factor Authentication is a subset of Multi-Factor Authentication, it is a method of confirming a user's identity by using a combination of two different factors.

Zadara's implementation of 2FA utilizes the open TOPT protocol (https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm) that computes a one-time password (also known as “authentication token”) from a shared secret key and the current time  to support two-step authentication. This one-time password changes every 30 seconds.

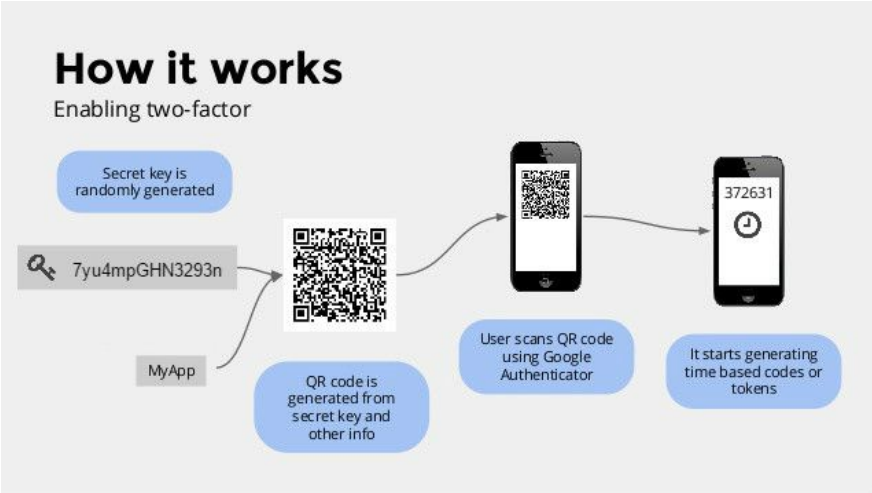
## Zadara 2FA Authentication

It is very common to use Google Authenticator to generate 2FA tokens on mobile devices. Several other applications, that utilize the same concepts such as Authy (https://authy.com/) or "Microsoft Authenticator", are also supported.

Applications like Google Authenticator implement the TOPT algorithm, which includes the following ingredients:

- Shared secret
- Input derived from current time
- Signing function

The main advantage of an app like Google Authenticator is that it resides on your phone, that is always with you. The app can be easily installed on Android or iOS, and doesn't need an Internet connection to work. While nothing is 100% proof, 2FA is the best form of additional protection. It is highly recommended to activate it for all Zadara applications.

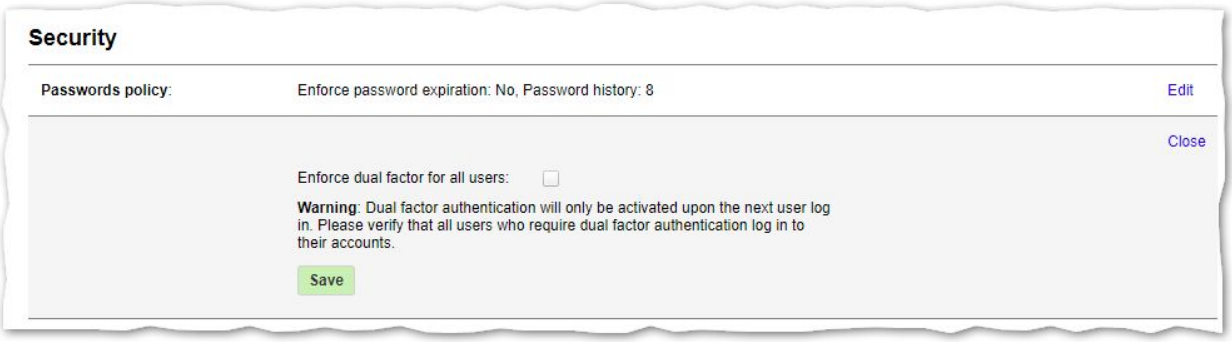



## VPSA Implementation and guidelines

- Each VPSA user can activate and use 2 factor auth for himself. The secret key is shared with the application via QR code that can be scanned by the mobile

device.


- A VPSA Administrator can activate “require 2FA” for all VPSA users, to mandate 2FA by all users.




Upon activating the 2FA for the VPSA Web Application, upon opening the VPSA GUI:

- User is confronted with a two fields login form -Username & Password.

- Upon successful basic login (username and password), an additional step will be required in order to complete the login, an authentication token:


- The Authenticator supplies the needs token