**Posted in:** Development (/spaces/127/sandpiper/forums/5366/development)

# Where to Store Secret Keys



**Doug Winsby (https://autocare.communifire.com/people/dougwinsby)**
3/28/2020

There's general agreement that "secrets" such as external API credentials, database connections and JWT signing secrets should not be hard-coded in the app or checked into version control. (This also applies, more generally, to **any** config variable)

Where there's not agreement is on the best practice for where to store (and set) these secrets. Most projects are now using the OS environment to set the secret as explained in "The Twelve-Factor App (https://12factor.net/config)".

But the article "Environment Variables Considered Harmful for Your Secrets (https://movingfast.io/articles/environment-variables-considered-harmful/)" explains why keeping this information in the OS environment is not really secure.

Some recommend keeping a "sample" configuration file (that is saved in version control) with instructions for the user to make a copy of that sample file for actual use (which is not saved in version control). Keeping the production file out of version control can be enforced with a `.gitignore` entry.

We've decided to take a hybrid approach that uses the "sample" file concept, but also allows you to "override" these secrets through environment variables if desired (some hosted solutions have good support for encrypted environments).

secrets (/spaces/127/sandpiper/searchresults?keyword=%22secrets%22&searchtags=1)

Reply (/forums/post?tid=5849&ReplyPostID=5850&SpaceID=127)

**Doug Winsby (https://autocare.communifire.com/people/dougwinsby)**
3/28/2020

We also added a default **minimum secret key length** of 32 bytes based on using the "HS256" algorithm as explained in this Auth0 excerpt (https://auth0.com/blog/a-look-at-the-latest-draft-for-jwt-bcp/) below (you can also make this value larger using the `min_secret_length` config file setting).

## Weak HMAC Keys

HMAC algorithms rely on a shared secret to produce and verify signatures. Some people assume that shared secrets are similar to passwords, and in a sense, they are: they should be kept secret. However, that is where the similarities end. For passwords, although the length is an important property, the minimum required length is relatively small compared to other types of secrets. This is a consequence of the hashing algorithms that are used to store passwords (along with a salt) that prevent brute force attacks in reasonable timeframes.

On the other hand, HMAC shared secrets, as used by JWTs, are optimized for speed. This allows many sign/verify operations to be performed efficiently but make brute force attacks easier (https://auth0.com/blog/brute-forcing-hs256-is-possible-the-importance-of-using-strong-keys-to-sign-jwts/). So, the length of the shared secret for HS256/384/512 is of the utmost importance. In fact, JSON Web Algorithms (https://tools.ietf.org/html/rfc7518) defines the minimum key length to be equal to the size in bits of the hash function used along with the HMAC algorithm:

> "A key of the same size as the hash output (for instance, 256 bits for "HS256") or larger MUST be used with this algorithm." - JSON Web Algorithms (RFC 7518), 3.2 HMAC with SHA-2 Functions (https://tools.ietf.org/html/rfc7518#section-3.2)

In other words, many passwords that could be used in other contexts are simply not good enough for use with HMAC-signed JWTs. 256-bits equals 32 ASCII characters, so if you are using something human readable, consider that number to be the minimum number of characters to include in the secret. Another good option is to switch to RS256 or other public-key algorithms, which are much more robust and flexible. This is not simply a hypothetical attack, we have shown that brute force attacks for HS256 are simple enough to perform (https://auth0.com/blog/brute-forcing-hs256-is-possible-the-importance-of-using-strong-keys-to-sign-jwts/) if the shared secret is too short.

minimum_length_secret (/spaces/127/sandpiper/searchresults?keyword=%22minimum_length_secret%22&searchtags=1)

Like

Reply (/forums/post?tid=5849&ReplyPostID=5851&SpaceID=127) Answer

**Luke Smith (https://autocare.communifire.com/people/autopartsource)**
3/29/2020

Doug, I agree with your conclusions and approach.

Like

Reply (/forums/post?tid=5849&ReplyPostID=5853&SpaceID=127) Answer

Page 1 of 1 (3 items)