**HMAC Message Digest Step:**

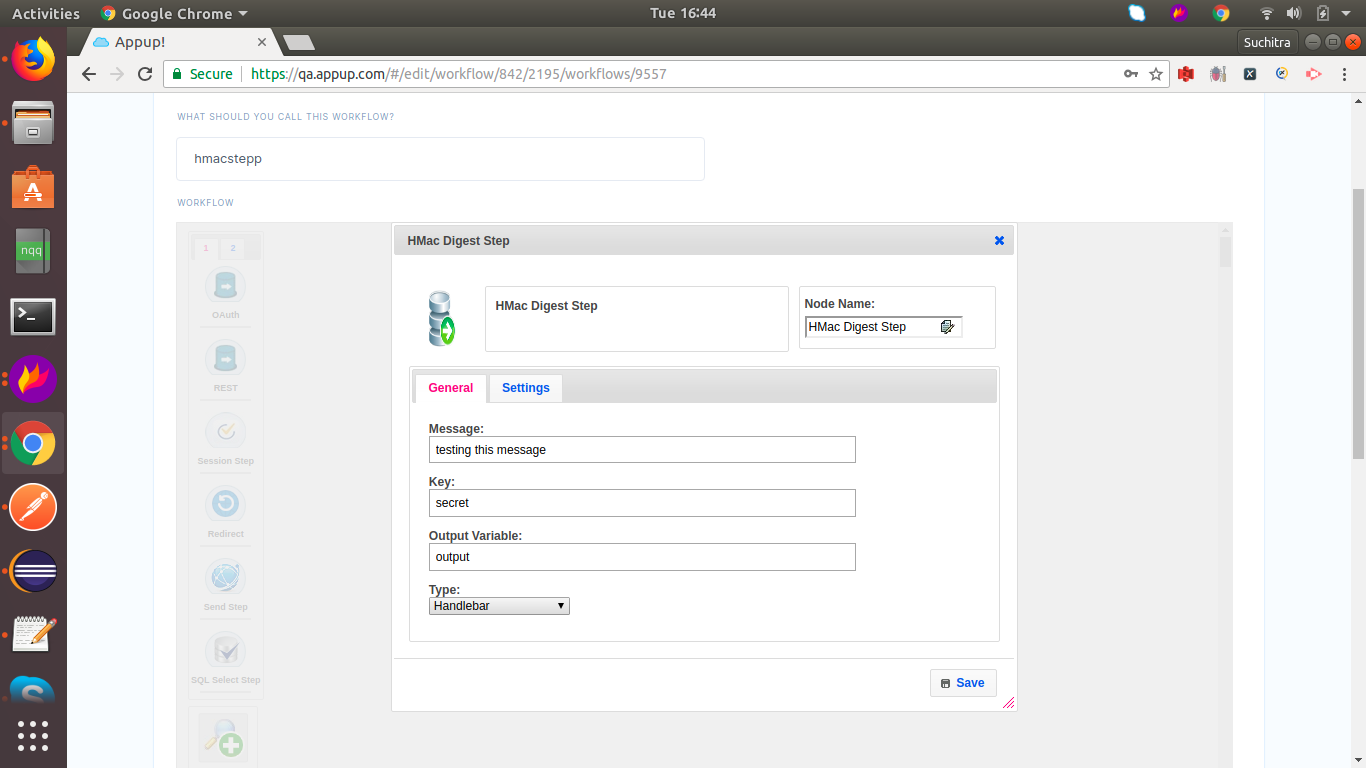
(**HMAC-Hash-based message authentication code**) is a mechanism for calculating a message authentication code involving a hash function in combination with a secret key. This can be used to verify the integrity and authenticity of a a message.

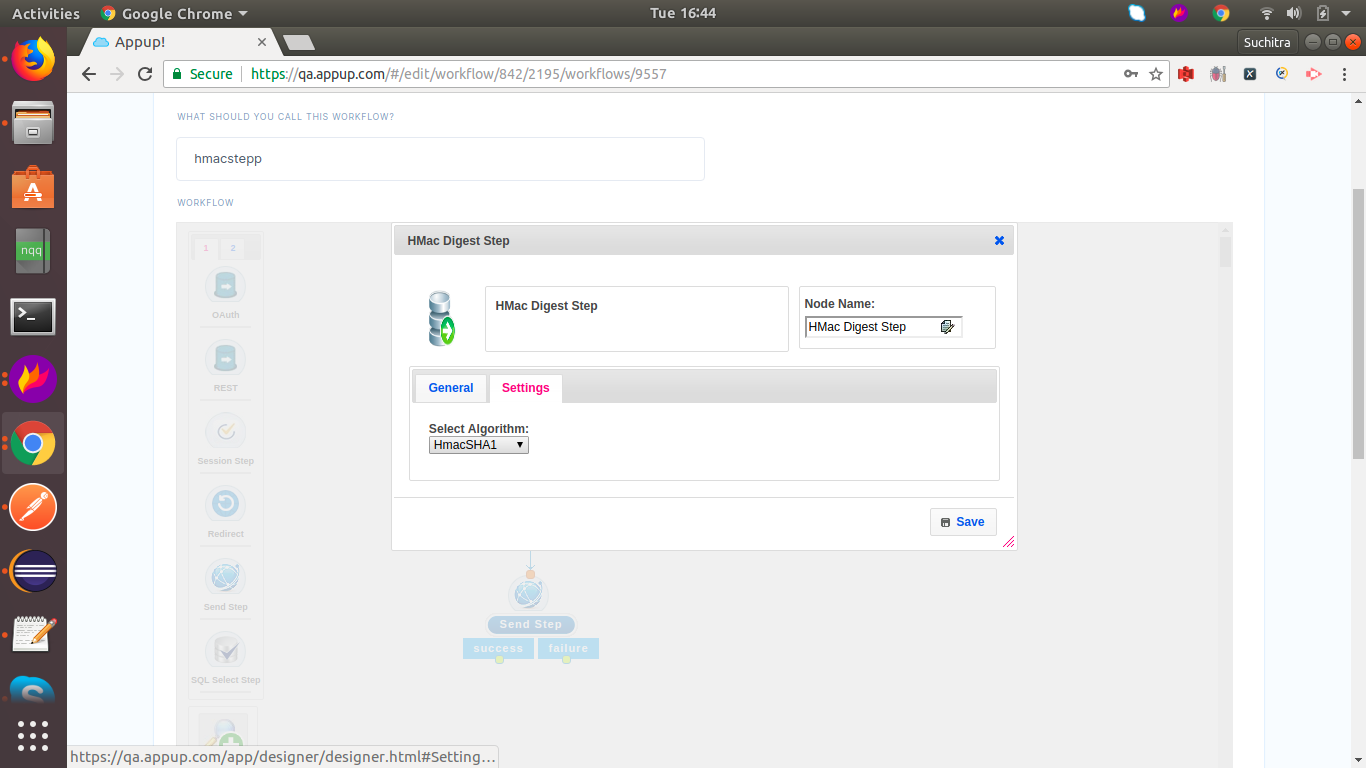
A message authentication code (MAC) is produced from a message and a secret key by a MAC algorithm

**Workflow:**

In the workflow required message has to be provided along with the secret key. These both are considered as inputs. There are different hash mac algorithms which are used to authenticate it.

Please check the below screenshots how to configure it.





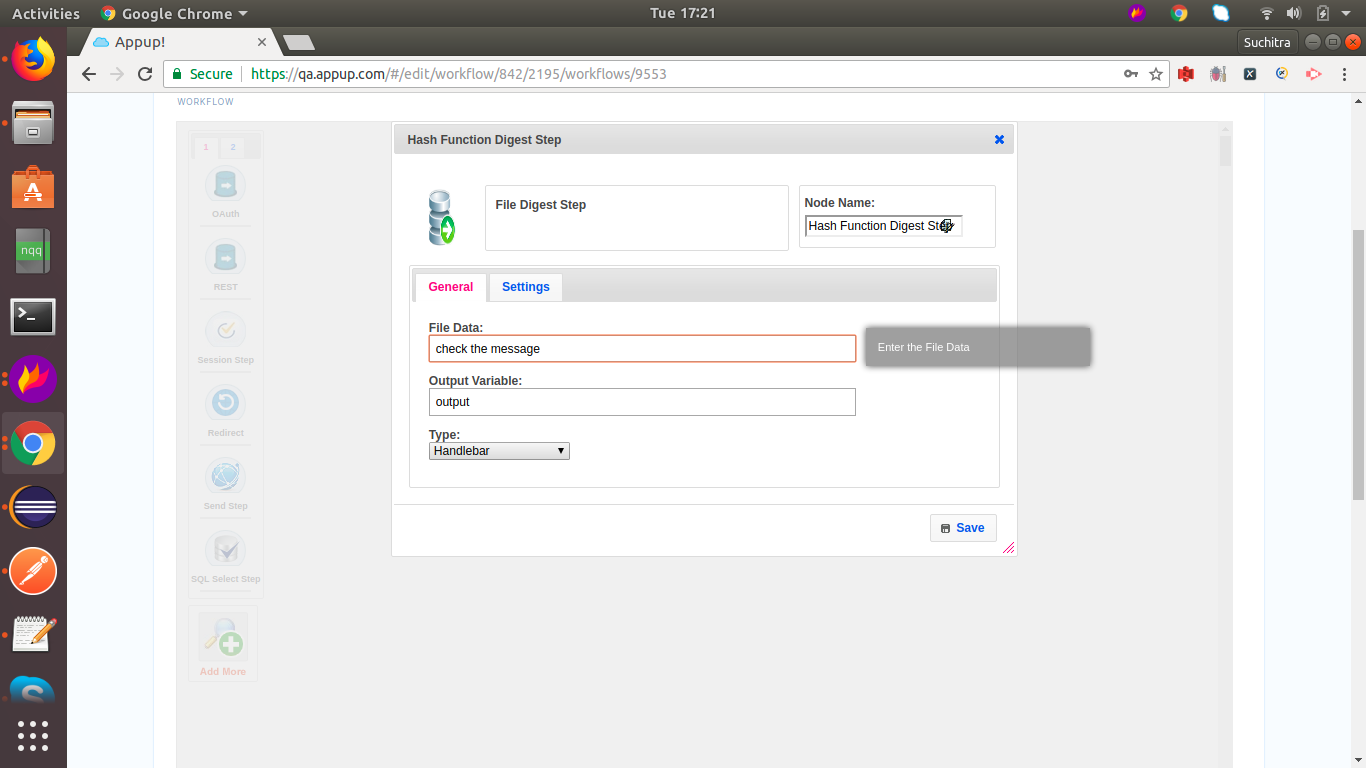
**Hash Function Message Digest Step:**

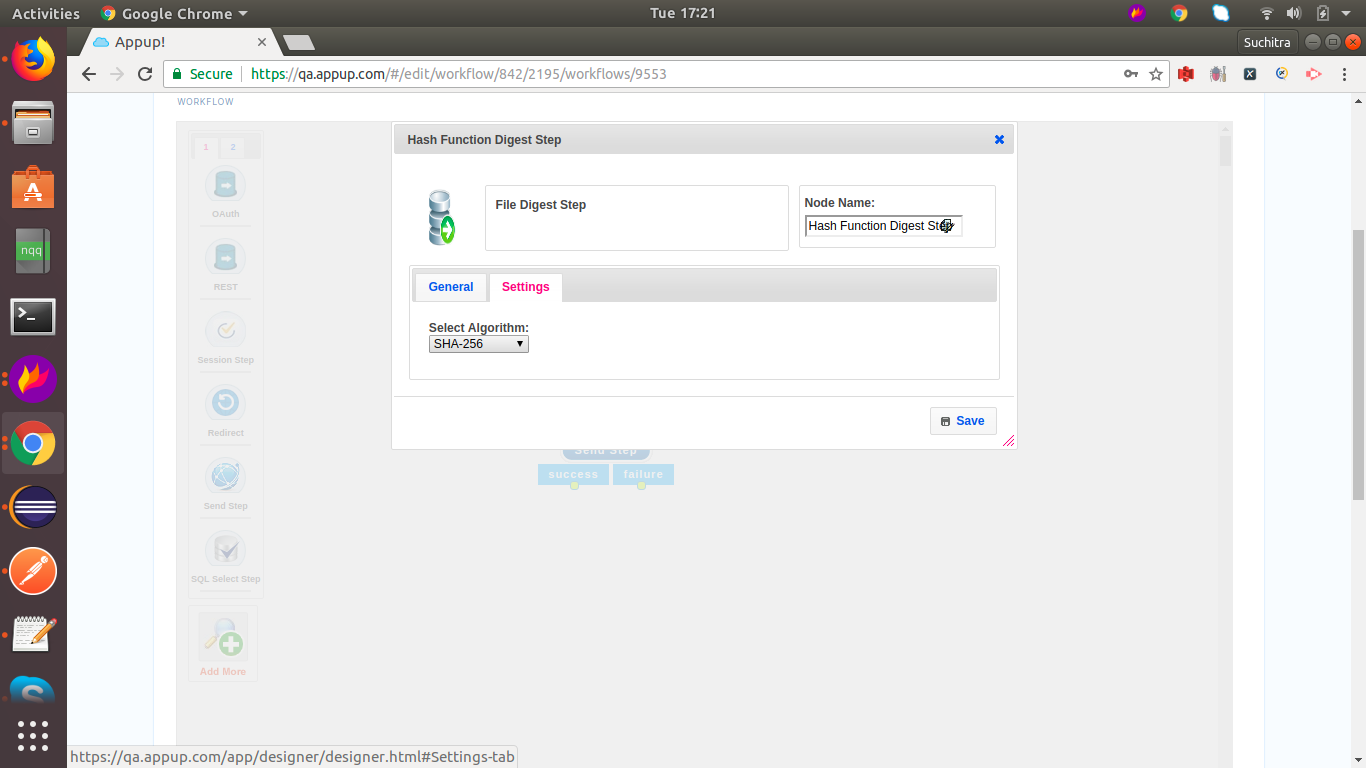
Hash function digest step usually considers the message and uses hash algorithm to produce the authentication code.

The main difference between hash function message digest and hmac message digest is in Hmac it uses a secret key which we provide in order to produce a authentication code. But in hash function message step it uses only algorithm to authenticate.

**Workflow:**

Please check the screenshots to configure the workflow





Postman links:

<https://www.getpostman.com/collections/dcd178895ea8bafa00e0>

Video links: