**CWE authentication manual code review**

The code for authentication is well structured. Comments and docstrings are used to explain the code. Looking at the auth\_store.py file, creating the new user, adding credentials, removing user, updating credentials, activating, and deactivating users is done properly. Proper use of async, assert, and await keywords is done. Using these keywords helps program to be synchronous and waits for the other callback function to complete its existing loop thus, avoiding the inconsistency in the storage. Exception handling in auth\_store.py could have been used for each function. For example, Exception handling for creating new user can be added. Though, exception handling for providing wrong group id is implemented. Removing the user is done by pop operation on the user id but other credentials should also be removed.

Looking at the \_init\_.py which is used to provide an authentication layer for Home Assistant. Exception handling is used in necessary parts. Classes for invalid authentication error and invalid provider are left blank without any body. These classes could have included the count for the invalid authentication from same Ip address so that, multiple log-in attempts from same Ip could be banned.



In providers, \_init\_.py the authentication provider functions and multifactor authentication provider function are defined. **CWE-287 – improper authentication** cannot be valid. As authentication is done properly. In CWE-287, remembering the cookies for the credentials is the problem, but in this code no cookies where remembered and also multifactor authentication is used. Exception handling for these functions is also implemented.



**CWE-291: Reliance on IP Address for Authentication** can be a valid CWE for Home Assistant. Home Assistant relies on the trusted network Ip addresses to bypass the log-in without any credentials. As per CWE-291, relying on the Ip address to bypass the log-in can be harmful. Ip addresses can easily be spoofed. At least the multifactor authentication should be implemented while allowing trusted networks to bypass the log-in. Code for trusted network is found under providers folder, trusted\_network.py.





Changing the return value to True can enable the multifactor authentication for trusted network.

**CWE-916: Use of Password Hash with Insufficient Computational Effort.** The CWE-916 specifies that using password hash function with insufficient computational effort can be harmful as many hash functions execute quickly with minimal overhead. CWE-916 suggests few hash functions that should be used such as bcrypt, scrypt, and PBKDF2 because they are all stronger than using salts with hash functions with very little computing overhead.

Home Assistant uses one of the suggested hash functions by the CEW-916 that is bcrypt.



The code for this is found in Homeassistant.py file which provides authentication.

**CWE-308: Use of Single-factor Authentication.** According to CWE-308, single-factor authentication can lead to unnecessary risk. Home assistant uses multifactor authentication which minimizes this risk. Home assistant provides max three trails for mfa.



## Code for this can be found at Core/[homeassistant](https://github.com/home-assistant/core/tree/dev/homeassistant)/[auth](https://github.com/home-assistant/core/tree/dev/homeassistant/auth)/[mfa\_modules](https://github.com/home-assistant/core/tree/dev/homeassistant/auth/mfa_modules)/\_init\_.py