Keycloak

Design

Operation

Understanding Password Policy with Keycloak and LDAP

Keycloak Password Policy

https://www.keycloak.org/docs/latest/server_admin/index.html#_password-policies

Password Policy at Realm level

Keycloak Password Policy has to be configured at realm-level.

Keycloak Password Policy Types

Kecloak provides the following Password Policies:

grafik.png

Policy Name	Description
Expire Password	The number of days for which the password is valid. After the number of days has expired, the user is required to change their password
Hashing Iterations	This value specifies the number of times a password will be hashed before it is stored or verified. The default value is 27,500
Special Characters	The number of special characters like '?!#%$' required to be in the password string
Not Recently Used	This policy saves a history of previous passwords. The number of old passwords stored is configurable. When a user changes their password they cannot use any stored passwords
Uppercase Characters	The number of upper case letters required to be in the password string
Lowercase Characters	The number of lower case letters required to be in the password string

Password Blacklist	This policy checks if a given password is contained in a blacklist file, which is potentially a very large file. Password blacklists are UTF-8 plain-text files with Unix line endings where every line represents a blacklisted password. The file name of the blacklist file must be provided as the password policy value, e.g. *10_million_password_list_top_1000000.txt*. Blacklist files are resolved against ${jboss.server.data.dir}/password-blacklists/ by default. This path can be customized via the keycloak.password.blacklists.path system property, or the blacklistsPath property of the passwordBlacklist policy SPI configuration
Minimum Length	The minimum length of a password
Regular Expression	Define one or more Perl regular expression patterns that passwords must match
Digits	The number of digits required to be in the password string
Not Username	When set, the password is not allowed to be the same as the username
Hashing Algorithm	Passwords are not stored as clear text. Instead they are hashed using standard hashing algorithms before they are stored or validated. The only built-in and default algorithm available is PBKDF2. See the Server Developer Guide on how to plug in your own algorithm. Note that if you do change the algorithm, password hashes will not change in storage until the next time the user logs in

Link

Thank you for this summary: https://www.janua.fr/understanding-password-policy-with-keycloak-and-ldap/

Troubleshooting

Links & Tools