When verifying users’ identity, the approach my policy that will be using user/pass as a base, and identifying user login point (state), and previous devices used to eliminate potential malicious users. When an attempted login happens, the user will be required to user a two-factor authentication app to log into their account, and if from an unused account or location, the user will also be required to use and additional authentication source, such as an email code to log in.

When user create passwords, this policy would use password salting and hashing to protect user passwords. On signup users will add their two-factor methods to their account. When resetting user passwords or authentication methods, this policy will employ a self-service password reset, allowing the user to change their password without administration. The reset will require the user to enter an old password and verify on both authentication methods. However, for resetting a authentication method, as long as the user is able to log into their account they will be able to change their authentication method.

| **Property** | **Username requirements** |
| --- | --- |
| Characters allowed | * A – Z * a - z * 0 – 9 * ' . - \_ ! # ^ ~ |
| Characters not allowed | * Any "@" character that's not separating the username from the domain. * Can't contain a period character "." immediately preceding the "@" symbol |
| Length constraints | * The total length must not exceed 113 characters * There can be up to 64 characters before the "@" symbol * There can be up to 48 characters after the "@" symbol |

| **Property** | **Password Requirements** |
| --- | --- |
| Characters allowed | * A – Z * a - z * 0 – 9 * @ # $ % ^ & \* - \_ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > * blank space |
| Characters not allowed | Unicode characters. |
| Password restrictions | * A minimum of 8 characters and a maximum of 256 characters. * Requires three out of four of the following:   + Lowercase characters.   + Uppercase characters.   + Numbers (0-9).   + Symbols (see the previous password restrictions). |
| Password expiry duration (Maximum password age) | * Default value: **90** days. * Maximum value: **180** days. |
| Password expiry notification (When users are notified of password expiration) | * Default value: **14** days (before password expires). |
| Password expiry (Let passwords never expire) | * Default value: **false** (indicates that passwords have an expiration date). * The value can be configured for individual user accounts |
| Password change history | The last password *can't* be used again when the user changes a password. |
| Password reset history | The last password *can* be used again when the user resets a forgotten password. |

Justinha, “Self-service password reset deep dive - azure active directory - microsoft entra,” *Self-service password reset deep dive - Azure Active Directory - Microsoft Entra | Microsoft Learn*. [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks. [Accessed: 30-Oct-2022].