The table below lists the password requirements. SSO and Multi-Factor Authentication (MFA) are supported through third parties. The location-based restriction is supported through some third parties. Genesys Cloud currently supports Google G Suite, Ping Identity, Microsoft Azure AD Premium, Microsoft Active Directory Federation Services (ADFS), OneLogin, OKTA, and Salesforce as Identity Providers.

* If you change your password requirements, existing users are not affected until they change their passwords.
* If a user enters a password that doesn’t fit your organization’s minimum and maximum requirements, the user receives an error message.
* The maximum length for a password is 400 characters.
* Genesys Cloud protects accounts from password-guessing scripts and other abusive behavior by locking out accounts after six unsuccessful consecutive login attempts. The lockout duration is five minutes.

**Table X - Genesys Cloud Password Requirements**

|  |  |
| --- | --- |
| Minimum Length | Minimum number of characters.  Note: The default minimum length for a password is 8 characters, including a default minimum of:   * 1 lowercase letter * 1 uppercase letter * 1 number * 1 special character |
| Minimum Letters | Minimum number of letters. Use this field if you allow your users to use any combination of uppercase and lowercase letters. |
| Minimum Lower Case Letters | Minimum number of lowercase letters. Use this field if you want to require your users to use some lowercase letters. |
| Minimum Upper Case Letters | Minimum number of uppercase letters. Use this field if you want to require your users to use some uppercase letters. |
| Minimum Numerals | Minimum number of numbers. |
| Minimum Special Characters | Minimum number of special characters.  Allowable characters: !”#$%&'()\*+,-./:;<=>?@[\]^\_`{|}~ |
| Password Expiration | Length of time in days before a password expires.  Notes:   * When you change this value, the change goes into effect immediately and affects all existing passwords. * Any existing passwords that are older than the number of days you specify must be changed immediately. * When a user’s password expires, that user must reset their password before they can log in to PureCloud. * If a user is logged in when their password expires, they will remain logged in. However, after they log off, the user must reset their password in order to log back in. |
| Minimum Age | Length of time in seconds before a user can change a password. |