Create Password Policies in ACES²

In support of the ACES² Security Policy and in response to your requests, we have improved the password security rules in ACES². You can now set password policies within ACES² to more closely align ACES² password policies with your school’s own password rules. The ACES² administrator in your admission office will be responsible for configuring your settings and unlocking and resetting passwords. You should also consider having a backup ACES² administrator in your office.

Create Password Security Settings

1. From **Utilities**, select **User**, then select **User** from the submenu.

2. Expand the Password Security Settings section.

3. Select the pencil icon to edit the section.
4. You can require ACES\(^2\) user passwords to include one, several, or all of the following options:

- **Contain an Uppercase Letter:** You can set the minimum number of uppercase letters required in the password.

- **Contain a Lowercase Letter:** You can set the minimum number of lowercase letters required in the password.

- **Contain a Number:** You can set how many numbers you require in the password.

- **Contain a Special Character:** You can set the number of special characters required in the password. (Examples of special characters are: `~!@#$%^*()_-+={}[]"',.?/)"

- **Disallow Username:** This is selected and cannot be deselected. Users cannot choose their username as a password.

- **Disallow First/Last Name:** Allow or disallow use of the user’s first or last name in the password.

- **Allow Spaces:** Allow or disallow the use of spaces in passwords. The use of spaces allows users to use passphrases as passwords (for example: My p@ssw0rd !s c0mplex).

- **Enforce Password History:** This determines the number of unique passwords that have to be associated with a user account before an old password can be reused. When you select this option, the field labeled Passwords Remembered becomes active and defaults to 1.
  
  - Enter the number of passwords you want ACES\(^2\) to remember in the Passwords Remembered field. This is the number of unique passwords ACES\(^2\) will require the user to create before they can reuse one. For example, if you enter 15 in the Passwords Remembered field, then after the user’s 15th password expires, their first password can be reused.

- **Enforce Minimum Password Length:** This is selected for you and cannot be deselected. The field labeled Minimum Number of Characters defaults to 8. The minimum password length for users must be at least 8 characters.

- **Enforce a Maximum Password Age:** This is the period of time (in days) that a password can be used before ACES\(^2\) requires the user to change it. When you select this option, the field labeled Maximum Number of Days becomes active and defaults to 1.
You can choose the number of days before users are prompted to change their password. If the Maximum Password Age is set to 15, then on the 16th day, users will be prompted to change their password.

When you implement a maximum password age, the following rule applies:

- All active user records will be updated to reflect that their last password update occurred on the date that the maximum age requirement was implemented. This will require users to change their password when the newly implemented password age is reached.

For example, if a school implements the maximum password age on 3/15/17 and sets the maximum age to 60 days, all user records will be updated to indicate that the last time they changed their password was on 3/15/17. This will require users to change their password again by 5/14/17 (60 days later).

- Enforce a Minimum Password Age: This is the period of time (in days) that a password can be used before ACES² requires the user to change it. When you select this option, the field labeled Minimum Number of Days becomes active and defaults to 1.

You can choose the number of days before users are prompted to change their password. If the Minimum Password Age is set to 15, then on the 16th day, users will be prompted to change their password.

You can set a password reminder to prompt users to change their password. When you select Include Password Reminder, the field labeled Number of Days before Expiration becomes active and defaults to 14. You can enter the number of days you want.

Upon login, users will see an on-screen message notifying them that their password will expire and must be changed within the set number of days. The reminder will appear every day, beginning with the day you establish.

Users can select Reset Password to change their password or select OK to continue to ACES². For detailed instructions, see the document titled How to Reset your Password.
Users can change their password before the expiration date by clicking **OK** or continue to use ACES² as one ordinarily would. If they have reached the expiration date, they must reset their password.

If users do not change their password prior to 11:59 PM Eastern Time on the expiration date, the password will expire, and they must ask the administrator to reset their password.

The maximum number of days for the password expiration reminder is 30.

5. If the school’s administrator enables any of the new settings, this will not affect the current ACES² users’ password settings immediately. The new settings become effective when
   - users change their password.
   - any of the new settings become applicable. The day you enable a setting is considered Day 1. For example, if you choose **Enforce Maximum Password Age** on the 1st of the month and choose 30 for the Maximum Number of Days, users must change their password on or before the 31st.

6. You must assign permission to a staff member to administer the password settings.
   - Only users with modify rights to Utilities.PasswordSettings can modify the log-on and password settings.
   - You can assign more than one user to this role.
   - The default will be “no access.” If you are the ACES² administrator at your school, you can grant permission to yourself or another staff member.