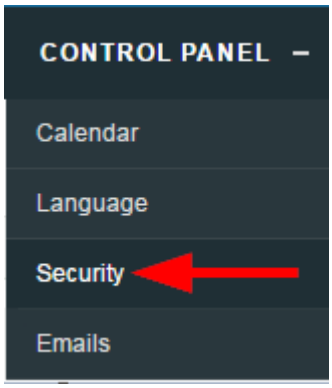
Password Security

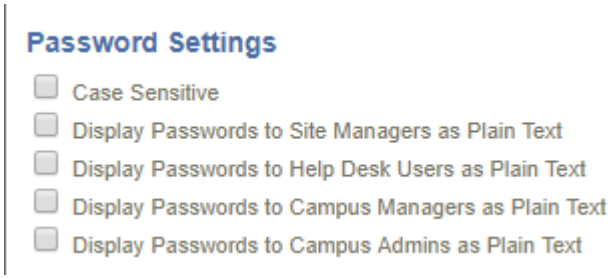
Site Managers can customize system password settings, such as requiring passwords with a minimum length. When users create their passwords, they will need to follow the requirements that you set up. If any security settings are altered to require a higher security, existing users will only be forced to update their passwords if the site is setup to enforce password security rules on login.

Password Settings

1. Log in with a Site Manager account.
2. Select **Security** under Control Panel in the main navigation menu.



3. Select the desired settings.



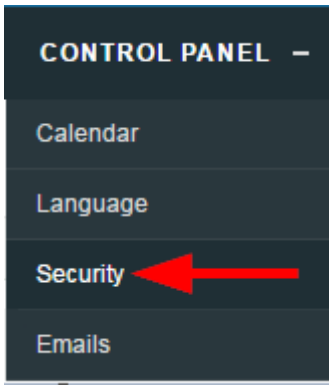
4. Choose **Case Sensitive** to require that passwords discriminate between uppercase and lowercase letters instead of allowing for either.
5. Choose which user types (if any) are allowed to view passwords as plain text. Plain text means that the stored passwords are unencrypted and can be easily read by the user types selected.
6. **Save**.

Systems that have encrypted passwords cannot display passwords as plain text to all of the user types shown above.

Password Strength

Site Managers can customize the requirements necessary for user passwords to strengthen the security for them. It is advised to balance the security of the password with consideration for the level of complication this will add for your users. Altering these settings will not affect existing users until they attempt to change their passwords.

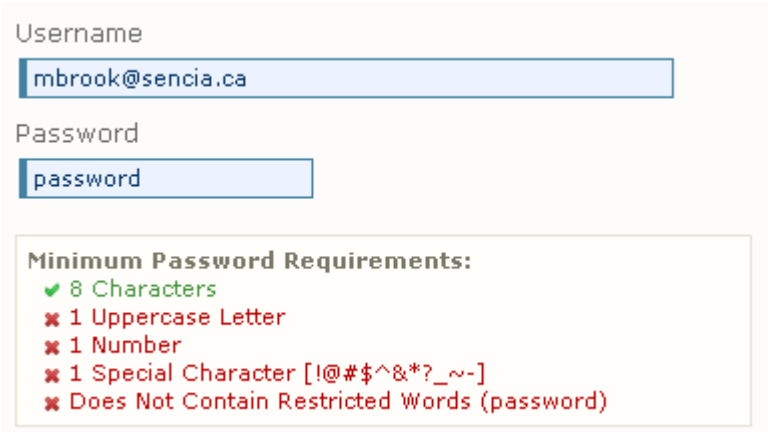
1. Log in with a Site Manager account.
2. Select **Security** under Control Panel in the main navigation menu.



3. Enter a minimum number into the field next to each selection for the password requirement. For the lower case and upper case options, the Case Sensitive option is required for this selection. See Password Settings.

4. **Save**.

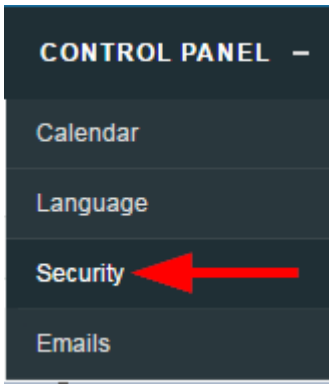
Password requirements display when a user creates a password. They are also visible from the user's profile page. Green lettering and a check mark indicate that the password meets requirements. Red lettering and an X indicate that the password does not meet requirements. The example below shows a user with both met and unmet password requirements.



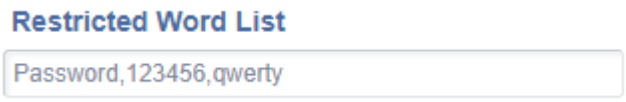
Restricted Word List

Site Managers can define characters, words, and phrases that cannot be used in passwords.

1. Log in with a Site Manager account.
2. Select **Security** under Control Panel in the main navigation menu.



3. Enter all restrictions into the field. Each entry much be seperated by a comma, without spaces.This feature ignores upper and lower case. An entry of 'cat' would not let users create passwords such as 'cat,'123Cat!', 'catalogue$$8', 'cattleprod'.

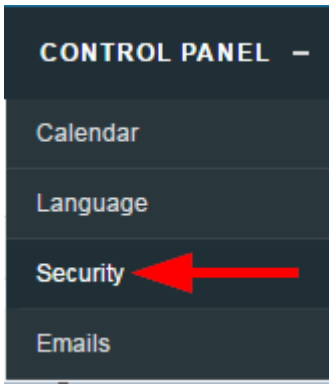


4. **Save**.

Forgot Password

Site Manager can define how the system will prompt users who select the Forgot Password link or who fail at their attempts to log in multiple times in a row.

1. Log in with a Site Manager account.
2. Select **Security** under Control Panel in the main navigation menu.



3. Select one option under Forgot or Change Password Email Option Setting.
    - **Change Password (Random) –** Activate this to email the user a new random password.

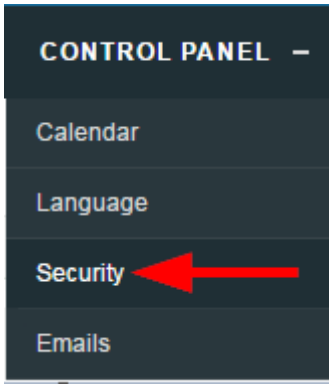
- **Forgot Password –** Activate this option to email the user instructions for recovering their password.

4. **Save**.

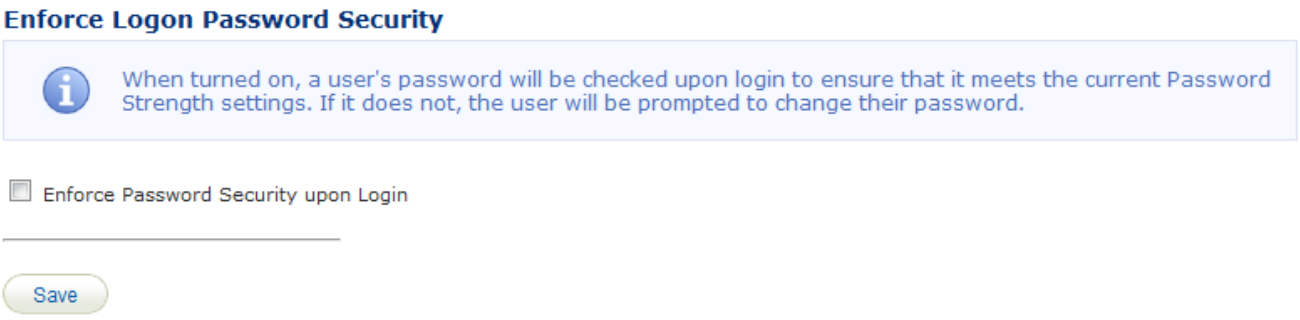
> Systems that use the Forgot Password link on the log in page trigger the option selected above when the link is selected.

Enforce Logon Password Security

1. Log in with a Site Manager account.
2. Select **Security** under Control Panel in the main navigation menu.



3. Enable **Enforce Logon Password Security** to check user's password upon login to ensure that it meets the current Password Strength settings. If it does not, the user will be prompted to change their password.



4. **Save**.