Passwords	
Send password emails from	Sets the email address from which password recovery emails will be sent.
Password format	Sets the format that the system uses to store user passwords. The passwords can either be secured using a cryptographic hash function or saved in plain text (not recommended). See Setting the user password format for more information. The recommended option that provides the best security is *PBKDF2*. If you change the password format setting, only future passwords are affected and existing passwords remain unchanged. You need to reset all passwords to store them in the new format. For this reason, it is recommended to set the appropriate format directly after the installation, before you create user accounts or allow users to start registering. **Note**: An empty string in the **UserPassword** field of the **CMS_User** database table is considered to be a blank password for both plain text and hashed password formats. If you forget the global administrator password, you can manually insert an empty value to reset it.
Password reset	
Reset password page URL	Sets the URL of the page where users can change their password after they submit a password recovery request. The **Reset password** web part must be placed on the specified page to ensure that users can set a new password. The value of this setting is used by the administration interface logon page and inherited by individual **Logon form** web parts if their own **Reset password page** property is not set. If empty, the **~/CMSModules/Membership/CMSPages/ResetPassword.aspx** default page is used.
Reset password interval	Sets the length (in hours) of the time interval during which users will be allowed to change their password after submitting a password recovery request. After the specified amount of hours, the link in the password recovery email will expire and become invalid.
Send email with password reset confirmation	Indicates whether the system sends users an email confirmation message of their password change. This setting is enabled by default.
Password expiration	
Enable password expiration	Indicates, if user's passwords should be valid only for the number of days specified in the following setting. If disabled, users' passwords never expire.
Password expiration period (days)	Specifies the number of days after which the users passwords become invalid.
Password expiration behavior	Specifies the behavior of the system after a user's password becomes invalid. See Password expiration for more information.

Password expiration warning period (days)	Specifies the number of days for which should be a warning message displayed before the user's password expires.
Send password expiration email	Indicates, if the system sends the users emails when their passwords expire.
Password policy	
Use password policy	Indicates if a security policy should be used to validate the passwords entered by users for their accounts. The details of the policy can be specified through the settings below. Passwords that do not meet the required conditions will be rejected. Enabling this setting does not change the passwords of existing users, it only adds requirements that must be fulfilled by new passwords.
Force password policy on logon	Indicates, if the system checks whether the users' passwords meet the configured password policy whenever the users try to log on. When the passwords do not meet the requirements, the users are forced to change the password. If disabled, the policy is applied only to the passwords of newly registered users.
Minimal length	Sets the minimum number of total characters required for user passwords.
Number of non alphanumeric characters	Sets the minimum number of non alphanumeric characters (i.e. any character except for numbers and letters) that must be present in a password in order for it to be accepted.
Regular expression	Can be used to enter a regular expression that will be used to validate user passwords. This regular expression is applied in combination with the other policy settings. For example: *^(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).*$* This sample expression would require passwords to contain at least one lower case letter, upper case letter and number. The minimum amount of characters would be determined by the remaining policy settings.
Policy violation message	Specifies a custom text message that will be displayed to users who attempt to enter a password which does not fulfill the requirements of the password policy. If left empty, a default message will be shown, informing about the minimum password length and number of non alphanumeric characters. If you specify a regular expression for passwords, it is recommended to describe its requirements in this message. If your site has multiple cultures (languages) assigned to it, you can enter a different message for each language via the **Localize** action.

Related pages

- Security model overview
- Securing user accounts and passwords
- Password strength policy and its enforcement