Login Limits & Lockouts

Admin users can configure lockout settings for Website users. Maximum number of failed logins, maximum retry time, and the lockout period can be set. If a user does not enter the correct password with the maximum failed login allowed, they will be locked out and cannot retry for a certain period. Admin users can unlock a locked user immediately in the CMS.
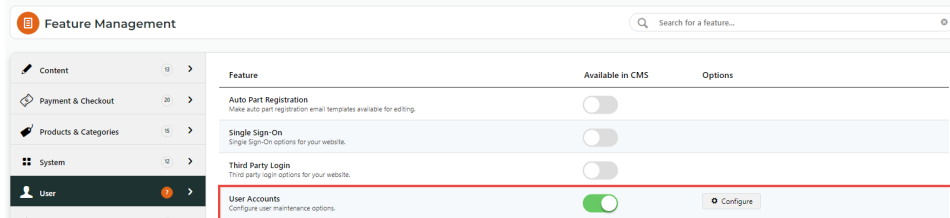

Step-by-step guide

To set Lockout Settings:

1. In the CMS, go to **Settings Feature Management User**.

2. Ensure **User Accounts** is toggled ON and click **Configure**.


3. Scroll down to **Lockout Settings**.

4. In **Login Max Retry Count**, enter the number of times a user can type an incorrect password before being locked out. Default: 3 times; 0 = unlimited number of tries.

5. In **Login Max Retry Time**, enter the time period (in seconds) within which the number of failed login attempts are counted towards a lockout. Default: 0 = 60 seconds.

6. In **Login Failed Lockout Time**, enter the time period a user will be locked out for. Default: 0 = 30 seconds.

7. When you have finished editing, click **Save** or **Save & Exit**.

Unlock a Locked User

Admin users can unlock a locked user immediately. This will bypass the Failed Login Lockout Time set.

1. *Go to **Users Website Users**.*

2. *Use the **Search** tool to find the user. A locked user will have an '**Unlock**' button in their row.*
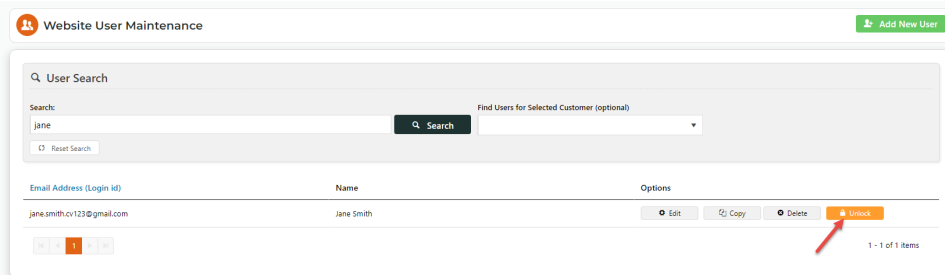
3. *Click the **Unlock** button. The User will be unlocked immediately. **NOTE -** This Unlock button will still display if the lockout period has passed and the user has not re-logged in.*

⊘ The Unlock button is also displayed in the User's Edit User page.

Related help

- [MS Active Directory Setup Guide](#)
- [Microsoft Azure AD SSO](#)
- [Users & Roles](#)
- [CMS Users](#)
- [Website Users](#)