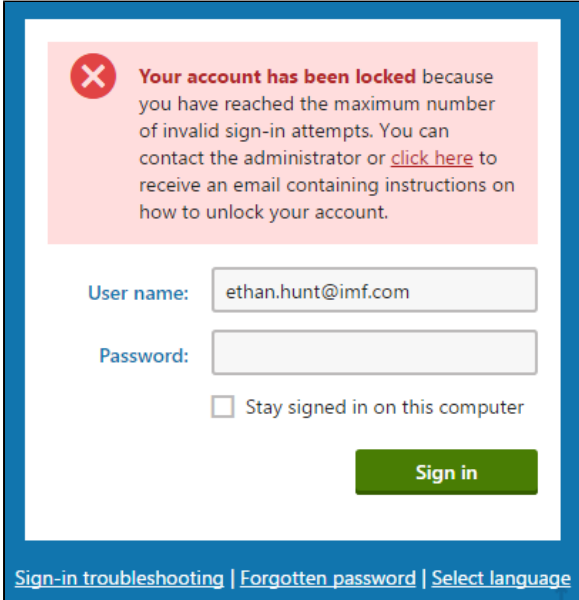


One of the most common threats to website security is stealing user accounts. To compromise an account, attackers use methods, which try to guess the password for that account, either by combining different characters or by selecting passwords from a dictionary.

This threat is eliminated by a **limit of invalid sign-in attempts**, which means that users will have their account locked after entering an incorrect password for the specified number of times.



The screenshot shows a login interface with a blue border. At the top, a pink message box with a red 'X' icon states: "Your account has been locked because you have reached the maximum number of invalid sign-in attempts. You can contact the administrator or [click here](#) to receive an email containing instructions on how to unlock your account." Below this, the "User name:" field contains "ethan.hunt@imf.com". The "Password:" field is empty. There is a checkbox labeled "Stay signed in on this computer" which is unchecked. A green "Sign in" button is at the bottom right. At the very bottom, there are links: "Sign-in troubleshooting | Forgotten password | Select language".

Limiting the number of invalid sign-in attempts

To configure the limit:

1. Open the **Settings** application.
2. Select the **Security & Membership -> Protection** setting tree item.
3. Configure settings in the **Invalid sign-in attempts** category:
 - **Maximum invalid sign-in attempts** – specified the number of possible sign-in attempts before the system locks the account and denies access. Type 0 to disable the account locking.
 - **Send unlock account email** – indicates whether an email notification should be sent to the user if their account is locked. Select the check box to send the notification.
 - **Unlock user account path** – specifies a path to a page where the user can unlock the account. If not specified, the system uses the default path: `~/CMSModules/Membership/CMSPages/UnlockUserAccount.aspx`

✓ For all protection settings, see [Settings - Protection](#).

4. Click **Save**.

The system now locks or does not lock user accounts according to your settings.

To display a friendly message to the users (as you can see on the picture above):

1. Open the **Settings** application.
2. Select the **Security & Membership -> Protection** setting tree item.
3. Enable the **Display account lock information message** setting.
4. Click **Save**.

If you do not enable the setting, the users will see only a general message that their sign-in attempt was unsuccessful without knowing that their account has been locked.

Users cannot sign in to a *locked* account. The global or site administrator has to unlock the account for them.



Using this protection may also lead to another security risk. If the users have easy-to-guess user names, then an attacker can block their accounts anytime by submitting wrong passwords with their user names on purpose.

Resetting the number of invalid sign-in attempts

When a user successfully signs in, the system automatically resets the number of invalid sign-in attempts to zero.

Administrators can also reset the invalid sign-in attempt counter manually:

1. Open the **Users** application.
2. **Edit** (✎) the given user.
3. Click **Reset** at the **Invalid sign-in attempts** field.

The system sets the number back to zero and unlocks the user's account (if the user has reached the limit).