Password Lockout

Table of Contents

Introduction

A password lockout is a security measure that temporarily restricts access to an account after a limited number of unsuccessful login attempts. When the threshold is reached, further login attempts are blocked for 30 minutes—or until the account is securely verified. This protection works alongside other safeguards such as secure password requirements and optional multi-factor authentication to help ensure only authorized users can access the platform.

Password lockouts help protect accounts from unauthorized access caused by automated password guessing, credential stuffing, or other suspicious login activity. By limiting repeated failed attempts, this control reduces the risk of account compromise, protects customer data, and supports industry-standard security practices, while still minimizing disruption for legitimate users.

An administrator user with appropriate permission has access to switch the password lockout feature on for their organization and to set the limit for failed login attempts before a user is locked out.

This feature applies to any user attempting to log in directly. It does *not* apply when using SSO to log in. Only administrators have access to unlock their users' accounts.

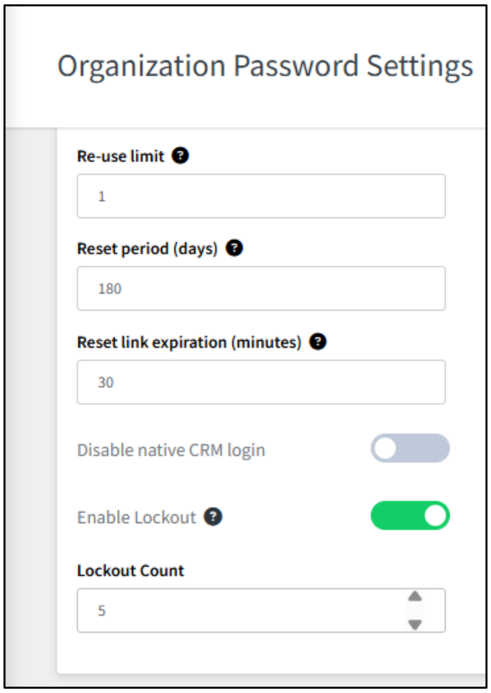
Setting the Lockout Threshold

An administrator with permission to set password settings can set the lockout threshold (the number of unsuccessful attempts a user has before their account is locked) for any user in their organization attempting to log in directly.

1. Navigate to **Organization Settings → Password Settings**.
2. Scroll to the bottom of the User Password Requirements section. Locate the **Enable Lockout** option and toggle the switch on.
    a. With this switch turned *off*, failed attempts are not counted. A user can make an unlimited number of attempts without being locked out.

   b. With this switch turned *on*, the Lockout Count field determines how many attempts a user has to log in.

3. In the Lockout Count field that appears below, enter a number for the threshold value. This value must be at least 1 and no more than 10.
4. Scroll up and click the **Save** button at the top of the User Password Requirements section.



Organization Password Settings

Re-use limit
1

Reset period (days)
180

Reset link expiration (minutes)
30

Disable native CRM login ○

Enable Lockout ●

Lockout Count
5

Lockout Observation Window

The time period during which the number of failed attempts is counted is the last 30 minutes.

Each time a user enters an incorrect password TE checks the number of consecutive failures in the last 30 minutes. If that number is equal to the threshold value, then the user is locked out of their account.

Example

Suppose the Lockout Count is set to 5, as shown in the example above. If a user attempts to log in at 9:00 am and mistypes their password, they have 4 more tries to enter it correctly. If they mistype their password 5 times, and it is not yet 9:30 am, they will be locked out and cannot make a 6th attempt.

If the user unsuccessfully attempts to log in at 9:00, 9:09, 9:20, and 9:28, they would be locked out if they try again before 9:30, but if the 5th attempt occurs at 9:31, they are not locked out because the first attempt was more than 30 minutes ago (there are only 4 failed attempts within the observation window).

Note

The system checks for *consecutive* failures. If a user successfully logs in, the lockout count is reset to 0, regardless of how many failed attempts they made.

Lockout Duration

Once a user reaches the lockout threshold, their account is locked for 30 minutes. During this time, the user cannot log in to their account, even by providing their correct, current password.

Note
Failed login attempts that occur during the lockout do *not* extend the duration of the lockout. The duration of lockout begins when the user trips the lockout threshold and ends 30 minutes later.

Unlocking an Account

There are 3 ways a locked account can be unlocked:

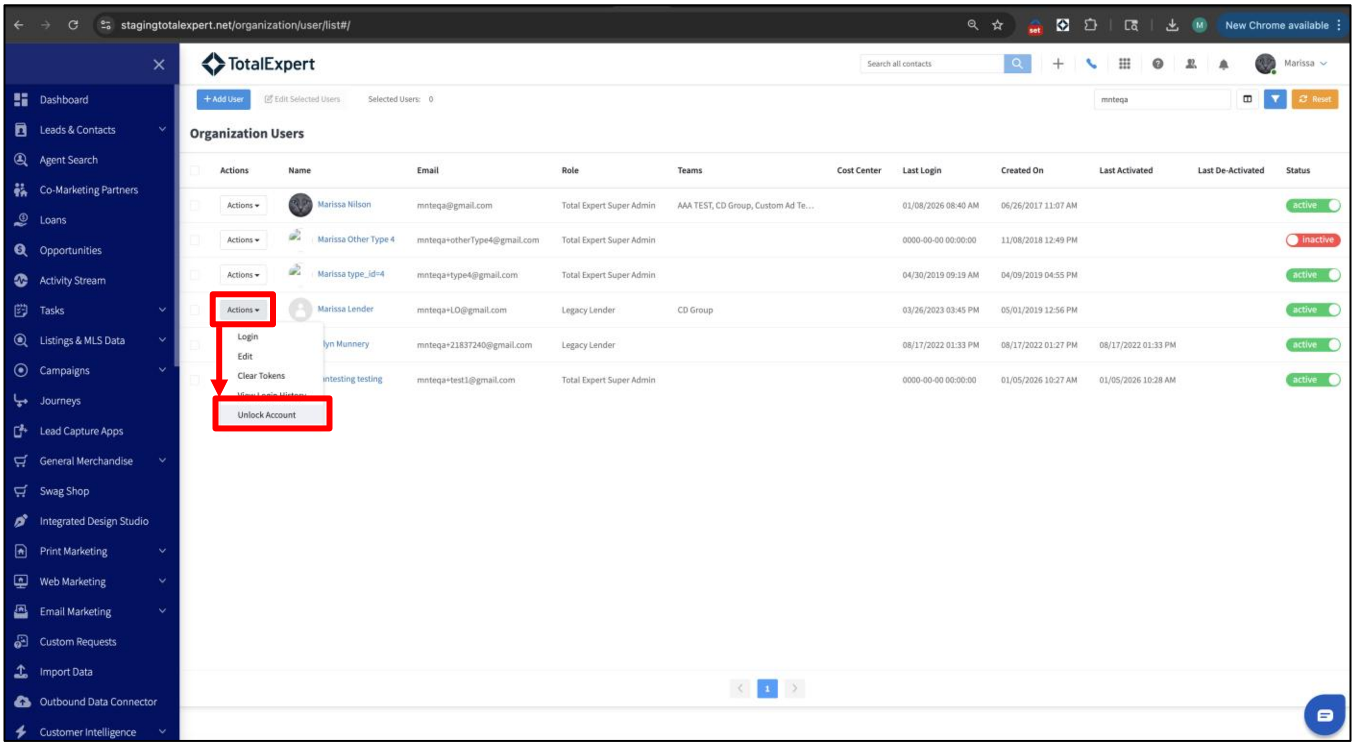
1. Expiration – After 30 minutes, the account is unlocked automatically, and the user can try to log in again.
2. Reset password – When a user resets their password via the existing reset password process, their account is unlocked immediately.
3. Administrator unlock – An administrator in the user's organization can use the process described in Administrator Unlock below to unlock the account.

Note
When an account is unlocked, the lockout count is reset to 0. This means the account will not lock again unless the user again reaches the lockout account threshold of failed attempts.

Administrator Unlock

Administrators with the appropriate permissions can unlock the account of a user in their organization.

1. Navigate to **Organization Admin → Users**.
2. Locate the locked user in the list and select **Actions → Unlock Account**.



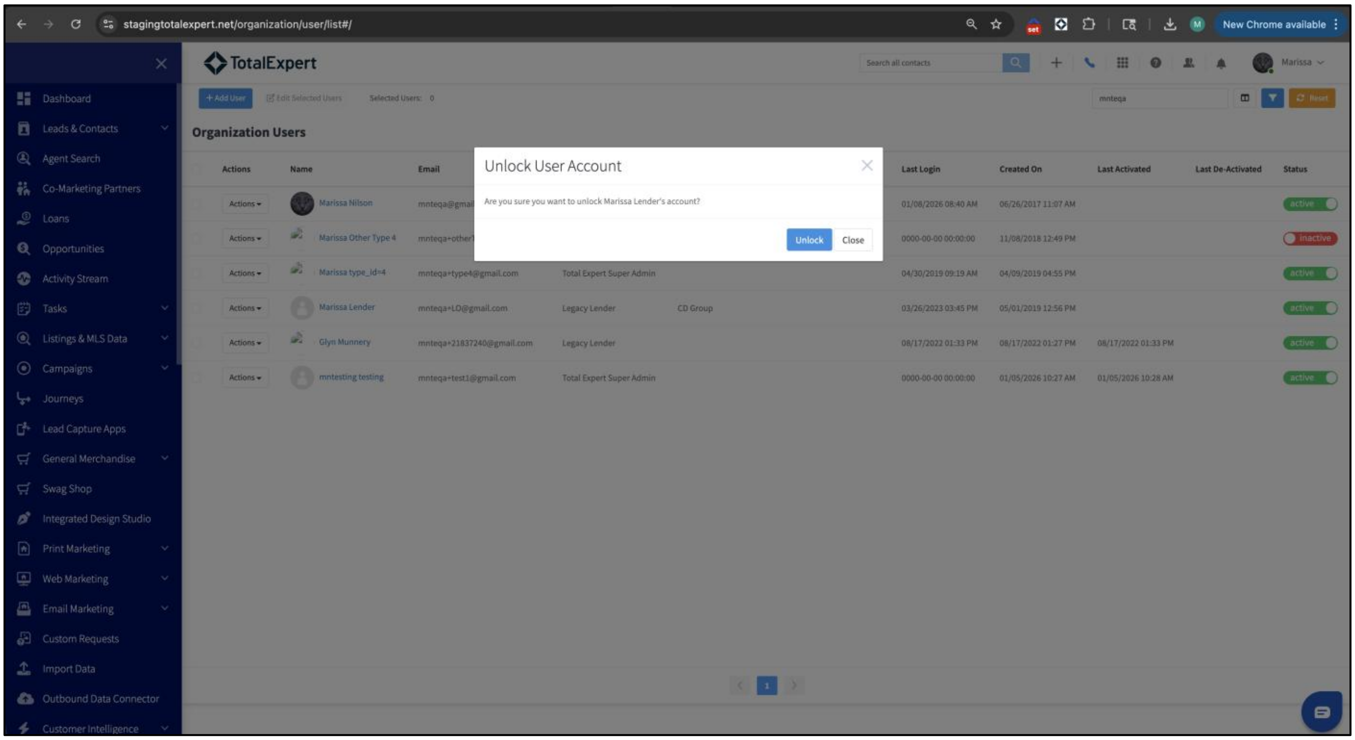
Selected Users: 0

mnteqa

Organization Users

Actions	Name	Email	Role	Teams	Cost Center	Last Login	Created On	Last Activated	Last De-Activated	Status
Actions ▾	Marissa Nilson	mnteqa@gmail.com	Total Expert Super Admin	AAA TEST, CD Group, Custom Ad Te...		01/08/2026 08:40 AM	06/26/2017 11:07 AM			active
Actions ▾	Marissa Other Type 4	mnteqa+otherType4@gmail.com	Total Expert Super Admin			0000-00-00 00:00:00	11/08/2018 12:49 PM			inactive
Actions ▾	Marissa type_id=4	mnteqa+type4@gmail.com	Total Expert Super Admin			04/30/2019 09:19 AM	04/09/2019 04:55 PM			active
Actions ▾	Marissa Lender	mnteqa+LO@gmail.com	Legacy Lender	CD Group		03/26/2023 03:45 PM	05/01/2019 12:56 PM			active
	lyn Munnery	mnteqa+21837240@gmail.com	Legacy Lender			08/17/2022 01:33 PM	08/17/2022 01:27 PM	08/17/2022 01:33 PM		active
	ntesting testing	mnteqa+test1@gmail.com	Total Expert Super Admin			0000-00-00 00:00:00	01/05/2026 10:27 AM	01/05/2026 10:28 AM		active

3. In the confirmation box, click the **Unlock** button.



Unlock User Account

Are you sure you want to unlock Marissa Lender's account?

Broker Users

Broker users see the same behavior when attempting to log in; however, when a broker user reaches the lockout threshold on 1 of their accounts, the lockout applies to *all* of their accounts. Similarly, when their account is unlocked (via any method) it unlocks all of their accounts simultaneously.