

# Der Fehler "Benutzerkonto gesperrt" bei der Anmeldung an der Blancco Management Console

Erstellungsdatum	Aktualisierungsdatum	Betroffene Version	Gefixte Version
23 Dec 2019	26 Feb 2020	Management Console 3.6.0 (und neuer)	N/A

## Beschreibung

Wenn Sie sich an der Blancco Management Console (BMC) oder Blancco Cloud anmelden wird die im Screenshot gezeigte Fehlermeldung "Benutzerkonto gesperrt" zurückgegeben.



Dies wird durch die Funktion "Brute Force Attack Prevention" der Management Console ausgelöst, die in BMC Version 3.6.0 implementiert wurde.

### Brute Force Attack Prevention:

- Wenn ein Benutzer versucht sich 10 Mal hintereinander mit einem falschen Passwort anzumelden wird der Account für 10 Minuten gesperrt.
- Gleichzeitig,
  - sendet die BMC eine E-Mail an die E-Mail-Adresse des Benutzers und teilt mit, dass das Konto gesperrt wurde.
  - sendet die BMC eine E-Mail an den Administrator, um über den Vorfall eines Brute-Force-Angriffs zu informieren. (Nur verfügbar von BMC 3.6.0 bis BMC 4.7.0)

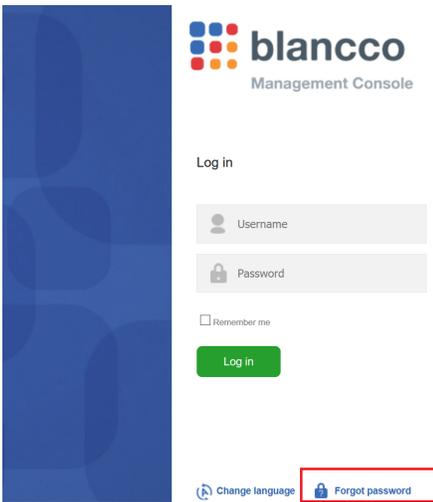
Beachten Sie, wenn Sie die lokale Version der Management Console verwenden, dass die SMTP-Servereinstellungen konfiguriert werden müssen damit die E-Mails gesendet werden können. Diese Einstellungen können nur vom Administrator unter der Registerkarte "Administration" konfiguriert werden.

## Schritt für Schritt Anweisungen

Sobald ein Benutzerkonto gesperrt ist müssen die 10 Minuten abgewartet werden. Das Konto kann auch vom Administrator nicht entsperrt werden.

Der Benutzer muss mindestens 10 Minuten warten, bis die Sperre automatisch deaktiviert wird.

Wenn der Benutzer das richtige Passwort vergessen hat, kann das Passwort über den Link "Passwort vergessen" zurückgesetzt werden.



Wenn entweder die E-Mail-Adresse des Benutzers oder die E-Mail-Servereinstellungen (SMTP) nicht ordnungsgemäß konfiguriert sind, muss der Benutzer den Administrator kontaktieren, um das Zurücksetzen des Kennworts zu beantragen.

## Überwachen von Brute-Force-Versuchen in den Logs (für Administratoren)

Wenn die Verhinderung von Brute-Force-Angriffen ausgelöst wird, schreibt die BMC mehrere Einträge im Zusammenhang mit der Aktion in das "main.log". Beispielsweise:

```
2020-02-26T13:37:16.162+02:00 [bmc-thread-2] INFO com.blancco.mc.spring.security.AuditLoggingAuthenticationFailureHandler - Login failure for user1 when attempting to log in from IP_ADDRESS
2020-02-26T13:37:19.978+02:00 [bmc-thread-3] INFO com.blancco.mc.security.BruteForcePreventionServiceImpl - Locking user user1; failed login attempts reached 10 while the threshold is 10
2020-02-26T13:37:19.989+02:00 [bmc-thread-3] INFO com.blancco.mc.service.communication.EmailServiceImpl - Send user locked email to the user's (user1) email (address: user@email.com); locked out for 10 minutes
2020-02-26T13:37:29.307+02:00 [bmc-thread-1] INFO com.blancco.mc.security.BruteForcePreventionServiceImpl - User user1 has been locked out, remaining lock out time: 590670 ms
```