

Account Lockout

Table of Contents

[Domain Configuration](#)

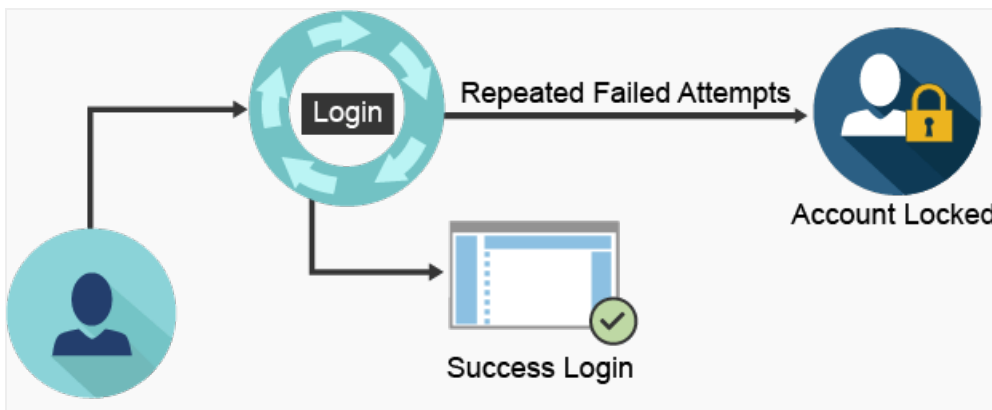
[User Configuration](#)

The automatic account lockout feature ensures that the hackers cannot find out a user's password by brute force method of trying out different passwords.

When enabled for the domain, users accounts can be automatically locked out when the number of unique invalid login attempts exceeds the given threshold in the specified interval.

Account lockout is checked when

- A user logs into the web client Baya
- A user logs into desktop or mobile POP, IMAP, SMTP, CalDAV clients
- A user logs into a desktop or mobile XMPP client.



From Admin Panel interface, you can view or update the Account Lockout related information for the domain or users.

Domain Configuration

[Steps](#)

[Account Lockout Properties](#)

Steps	Account Lockout Properties
Admin Panel > Domain name > Account Lockout	<ul style="list-style-type: none">• Enable Account Lockout.• Enable/ Disable unlock the account automatically.• Set the User Authentication Error Message.• Decide the Account Lockout Period.• Set Max Invalid Password Attempts.• Set Max Invalid Password Attempts Interval.

User Configuration

Steps	Account Lockout Properties
Admin Panel > Domain name > User name > Account Lockout	<ul style="list-style-type: none">• Decide the status of the account whether it is locked or not.
