



## How to Lock Out a User Account after Multiple Unsuccessful Login Attempts

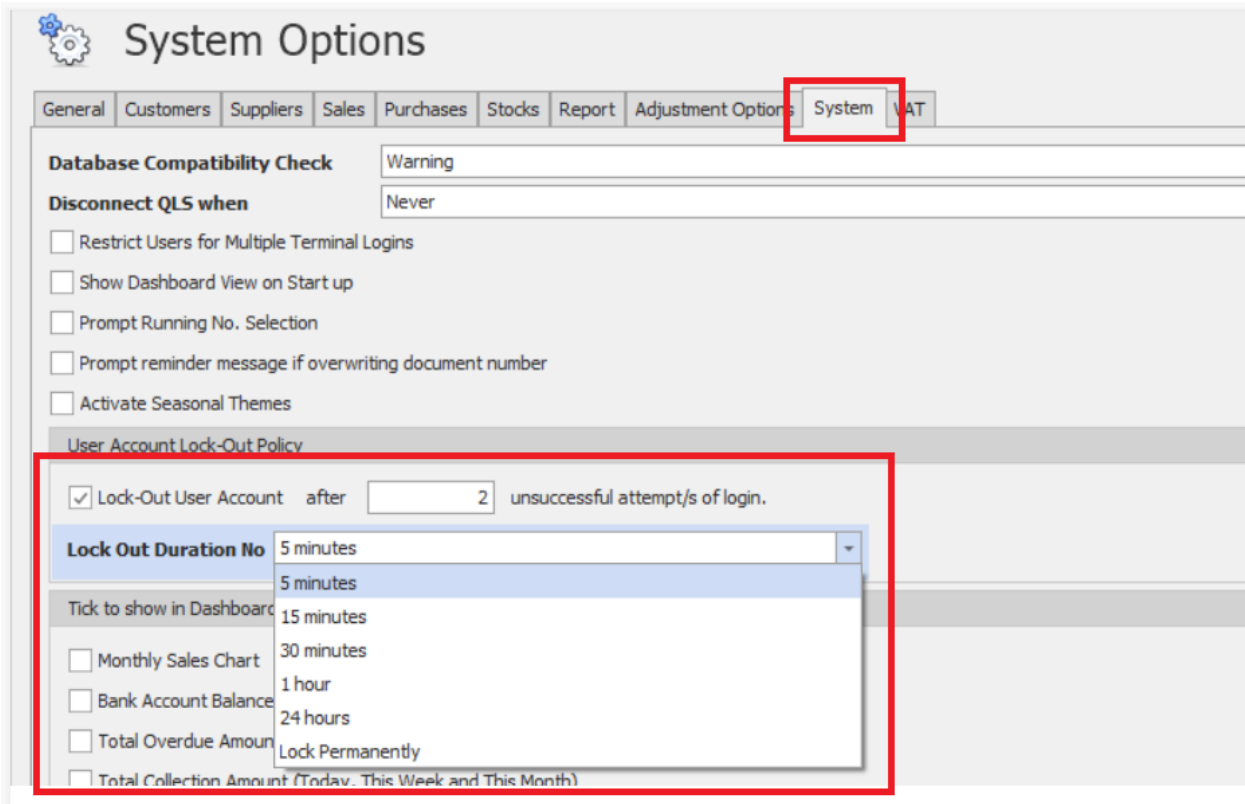
### Overview:

To provide control or setting in the system to restrict users from logging in after several failed attempts, in compliance with the BIR CAS - STANDARD FUNCTIONAL AND TECHNICAL REQUIREMENTS as stated "User identification codes are deactivated after unsuccessful attempts to sign on the computer."

### Procedure:

Go to Maintenance > System Options > System. Under User Account Lock-Out Policy, Tick 'Lock Out User Account after (Number of Attempts) unsuccessful attempt/s of login' and set the desired No. Of Attempts, by default, it is set to 2.

While for the 'Lock Out Duration No', select how many minutes or hours are needed for the user to wait before s/he can login and use the system again. The system also has an option to permanently prohibit the user from logging in.



**System Options**

General Customers Suppliers Sales Purchases Stocks Report Adjustment Options **System** VAT

**Database Compatibility Check** Warning

**Disconnect QLS when** Never

☐ Restrict Users for Multiple Terminal Logins

☐ Show Dashboard View on Start up

☐ Prompt Running No. Selection

☐ Prompt reminder message if overwriting document number

☐ Activate Seasonal Themes

**User Account Lock-Out Policy**

☒ Lock-Out User Account after 2 unsuccessful attempt/s of login.

**Lock Out Duration No** 5 minutes

5 minutes

15 minutes

30 minutes

1 hour

24 hours

Lock Permanently

**Tick to show in Dashboard**

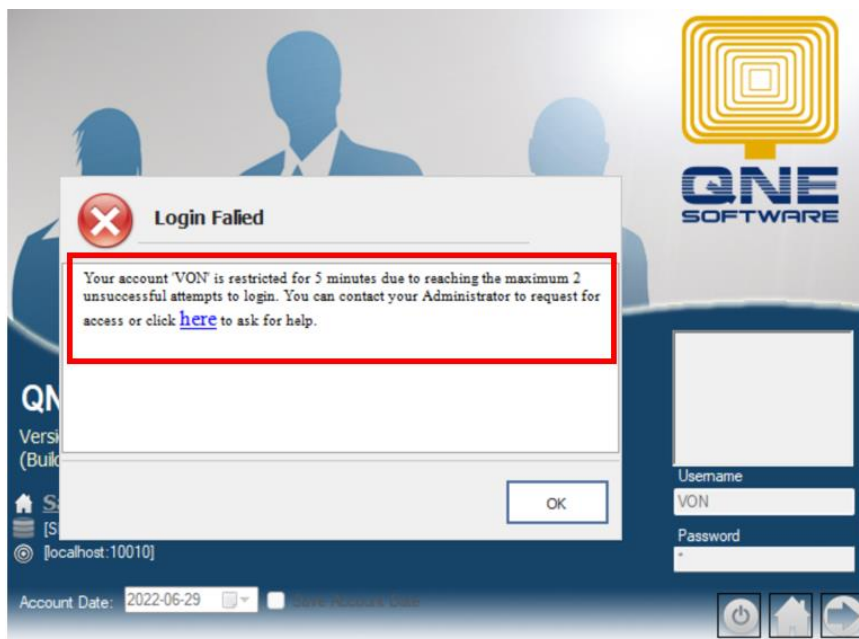
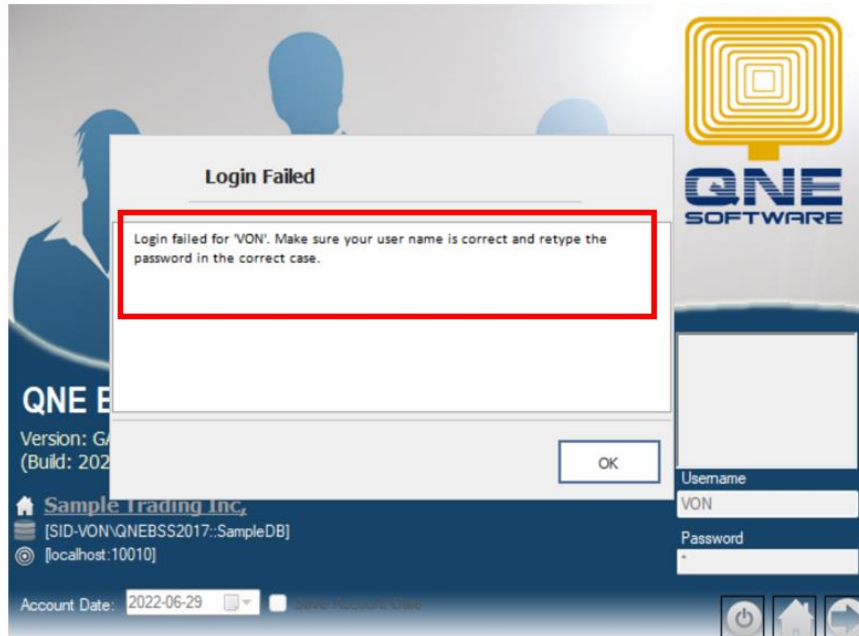
☐ Monthly Sales Chart

☐ Bank Account Balance

☐ Total Overdue Amount

☐ Total Collection Amount (Today, This Week and This Month)

Once the set number of unsuccessful login attempts has been reached, the account will be locked out for the duration set in the System Options.



**For further concerns regarding this matter, please contact support to assist you or create ticket thru this link <https://support.qne.com.ph>**