Application Note
AN_Password_Security:

Lockout after invalid passwords

1. Overview

MultiFlex controllers with firmware versions starting at **T036** can be set to lockout Modem, Trackster and Browser access after 5 incorrect passwords on any combination of user ids.

Password Lockout does not block access for on-site keypad users.

Browser users will be able to view the current state of the controller but will not be able to modify a locked-out controller's operation.

Modem and Trackster users will not be able to connect to a locked-out controller.

2. Lockout

Lockout ends at 7:00AM controller time.

Worst-case lockout time is therefore 24 hours for five incorrect passwords entered at 7:01 AM.

Lockout can be ended at any time by turning controller power OFF then ON, allowing on-site staff to restore remote access to a locked out controller.

The Lockout invalid password count is reset to 5 on every successful login.

Lockout is seldom used when controller access is limited to a few on-site users.

Lockout is applicable for users that are accessing the controller remotely via a VPN or for controllers that are connected to large on-site networks.

Password Guidelines:

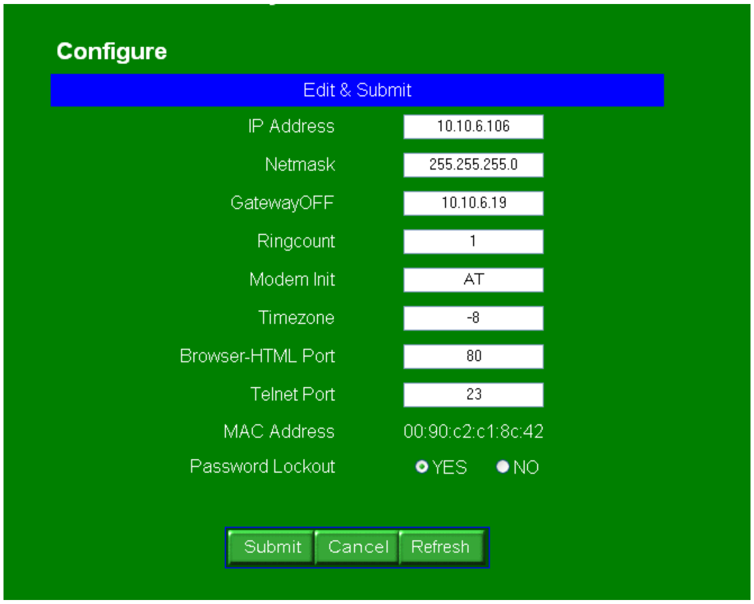
1. Change the **admin** and all seven of the user passwords from the factory defaults.
2. Set the **admin** password to differ from all user id passwords.
3. Changing the seven used ids does not necessarily make for added security since you cannot change the **admin** user id.
4. Limit your remote use of the **admin** password. If you are accessing the controller from the Internet using a VPN, use only your userid password.
5. Change your password regularly if you ever find your are locked out of a controller. It's an indication that someone else has been trying to access the controller.
6. If you are the only user, consider making all userid passwords the same. There's no practical reduction in security & it makes maintenance easier.

3. Setting the Lockout Option

The controller default is **Password Lockout** disabled, turned OFF.

You'll need to log on as **admin** to set the **Password Lockout**.
If you are logged on at another user id, you will be prompted for the **admin** password.

Connect to the controller using the browser and select **Communicate / Configure**
Set '**Password Lockout**' to **YES** and **Submit**



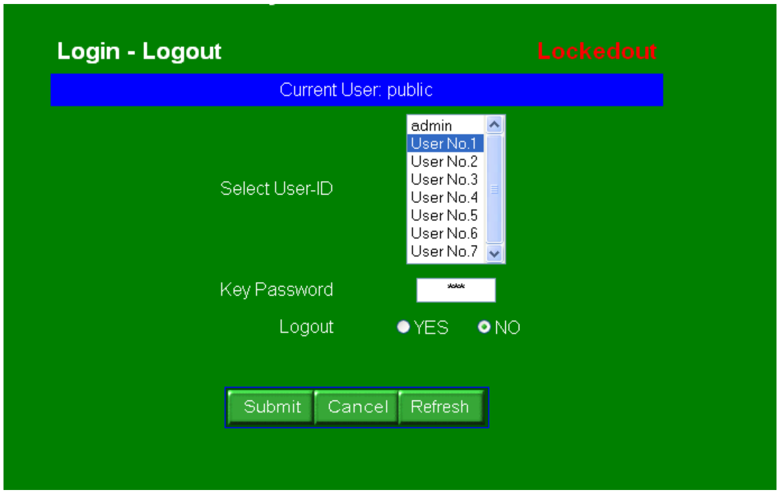
Configure

Edit & Submit

IP Address	10.10.6.106
Netmask	255.255.255.0
GatewayOFF	10.10.6.19
Ringcount	1
Modem Init	AT
Timezone	-8
Browser-HTML Port	80
Telnet Port	23
MAC Address	00:90:c2:c1:8c:42
Password Lockout	● YES ○ NO

4. Browser Lockout

Here’s what you’ll see when you attempt to log into a locked out controller:



Login - Logout

Lockedout

Current User: public

Select User-ID: User No.1

Key Password: ***

Logout ○ YES ● NO

You can still view current the controller state.

You just can’t log on and change anything until 7:00AM.