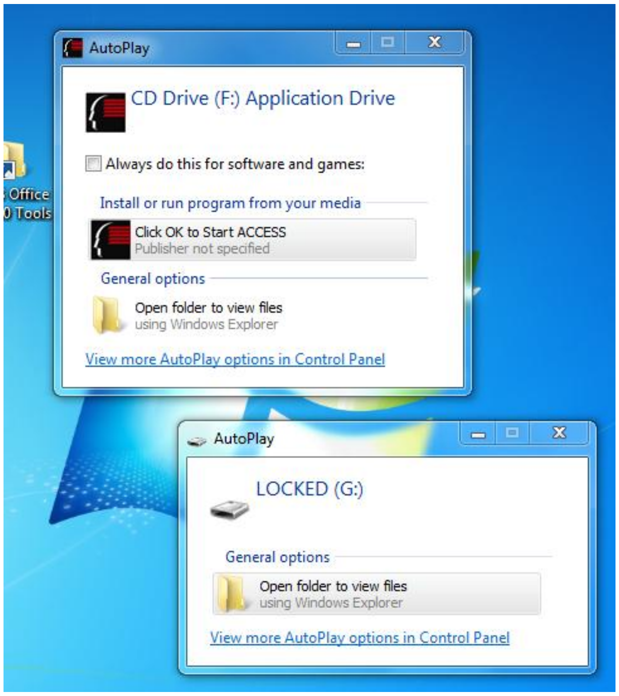
MXI USB Drive
Device Administrator Instructions

Version 2.0

FSSA Privacy & Security Compliance Office

Please read the MXI USB Drive User Instructions first.

1. Uncap and insert device in any available USB port.
2. The green light on the MXI Drive will be on, indicating that the drive has not yet been personalized. If the light is red, the device has already been set up and is locked.
3. Note: if your computer has Auto Play or Auto Run enabled, a screen similar to the following will appear when you plug in the MXI Drive:


AutoPlay
CD Drive (F:) Application Drive
☐ Always do this for software and games:
Install or run program from your media
Click OK to Start ACCESS
Publisher not specified
General options
Open folder to view files
using Windows Explorer
View more AutoPlay options in Control Panel
Office
0 Tools
AutoPlay
LOCKED (G:)
General options
Open folder to view files
using Windows Explorer
View more AutoPlay options in Control Panel

If it does appear, click on **Click OK to Start ACCESS**

Then go to Step 9

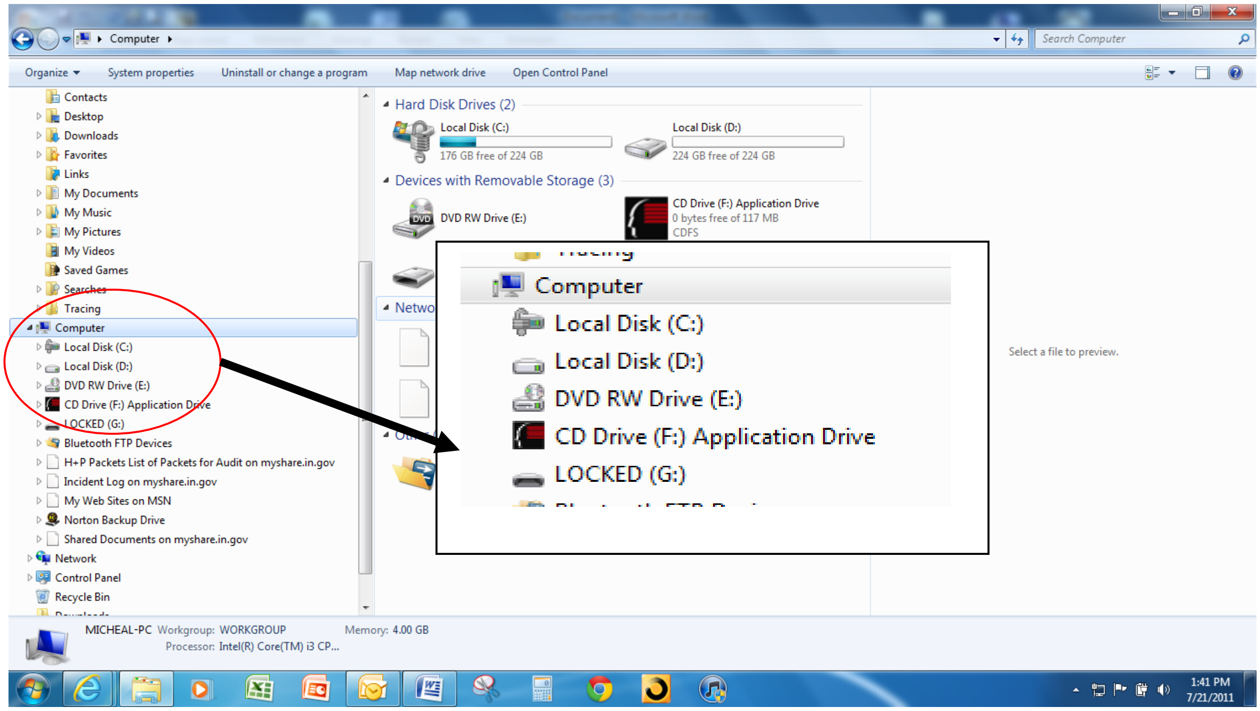
If it does not appear, go to Step 4

If the Locked drive also appears, just click on the **X** to close it.

You can do that before or after the above step.

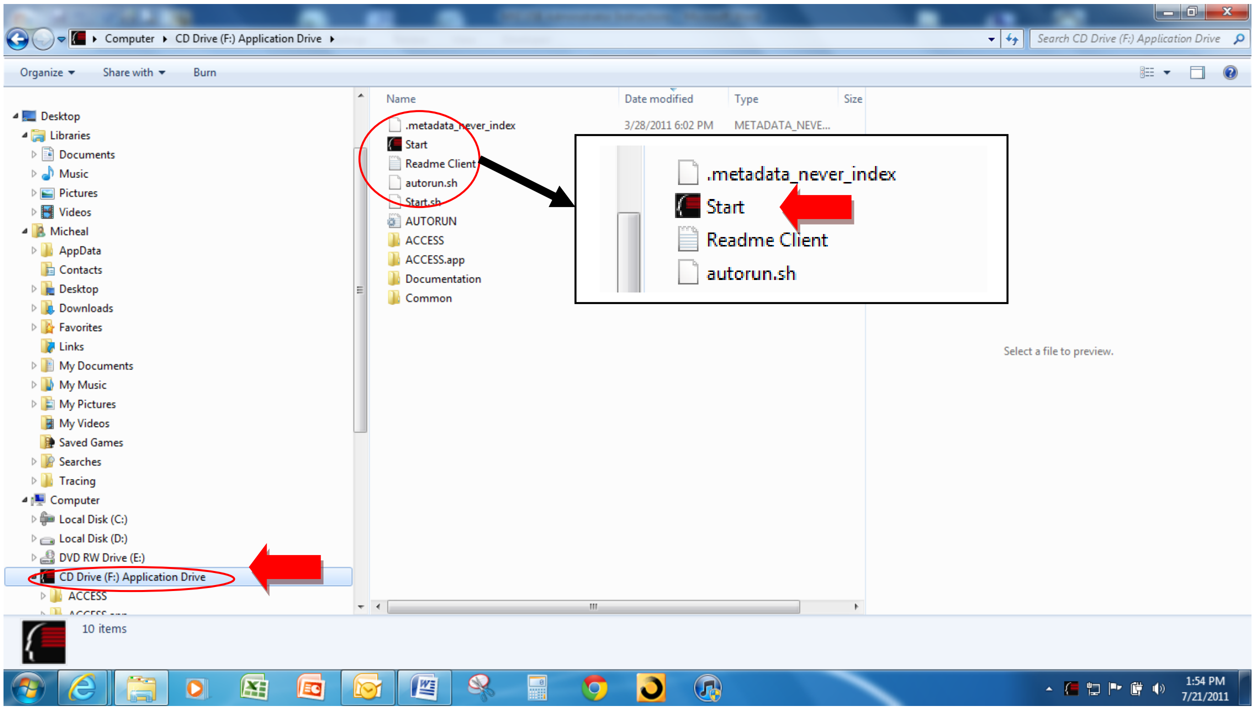
[Next Page]

4. Open Windows Explorer.
5. You will see the MXI Drive under Computer or My Computer: it has two partitions—*Application Drive* and *Locked*. The partitions display as drives F and G in this example; your drive letters may be different.

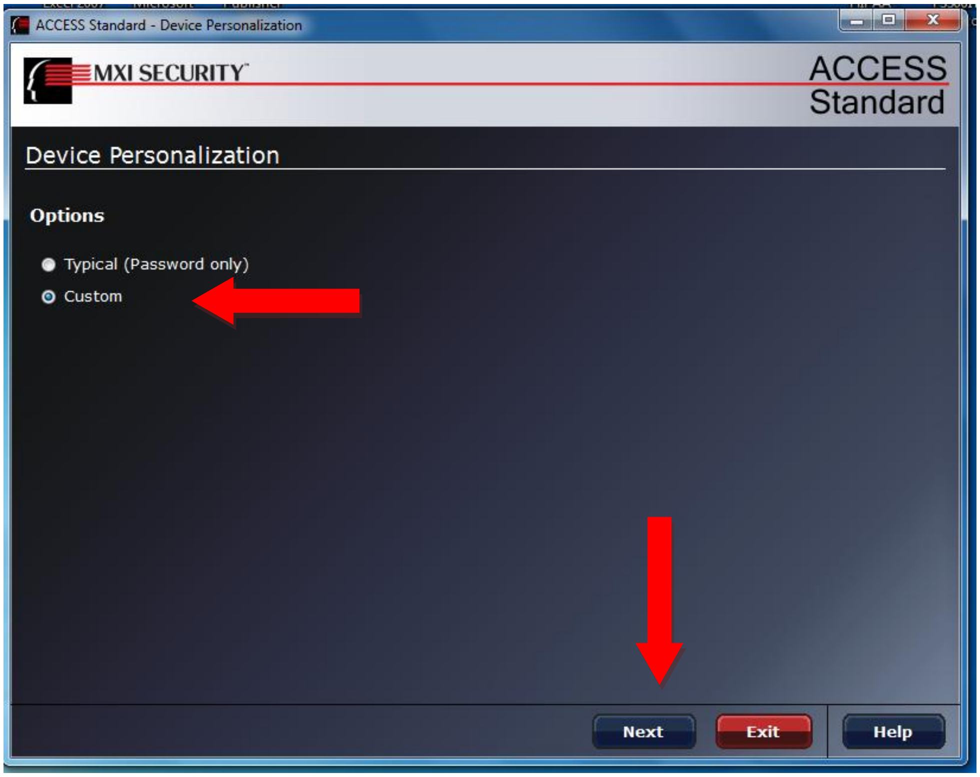


[Next Page]

6. Double click on the **Application Drive**
7. Double click on the **Start** icon



8. This will start the MXI ACCESS software: Device Personalization
9. Device Personalization Step 1: Click on **Custom**; then click **Next**


ACCESS Standard - Device Personalization

MXI SECURITY

ACCESS Standard

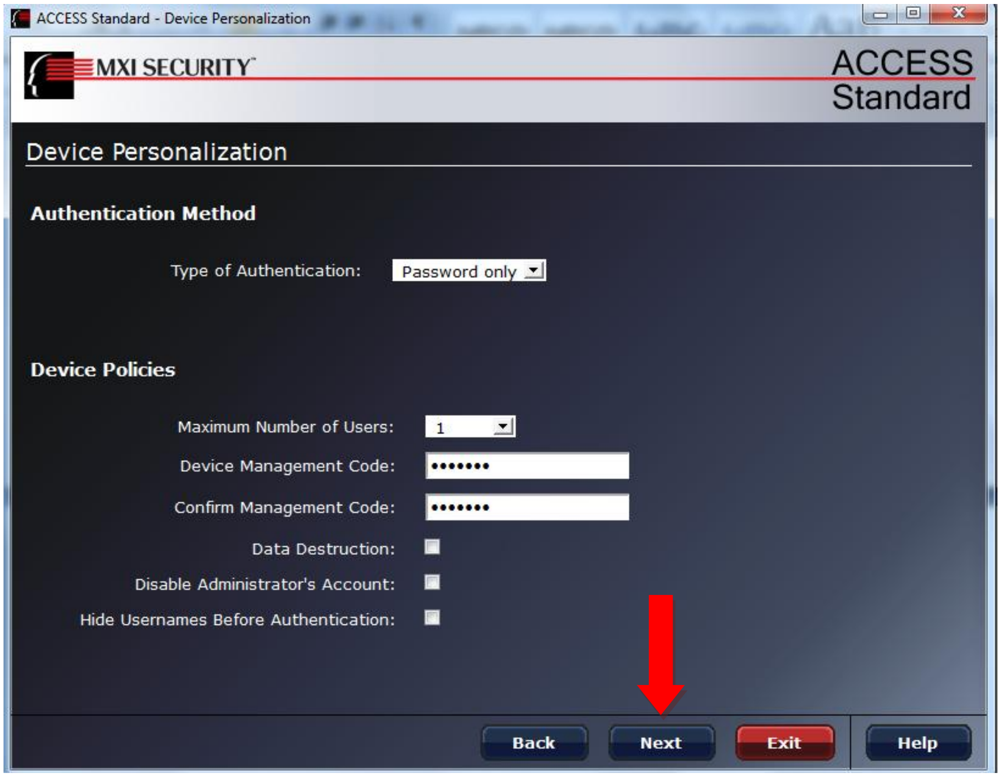
Device Personalization

Options

○ Typical (Password only)

● Custom

10. Device Personalization Step 2:
    a. Type of Authentication is to remain Password only
    b. Maximum Number of Users is to remain 1
    c. Device Management Code[1]: enter **RECYCLE** (all caps)
    d. Confirm Management Code: enter **RECYCLE** (all caps)
    e. Leave the last three items blank and click **Next**



Device Personalization

Authentication Method

Type of Authentication: Password only

Device Policies

Maximum Number of Users: 1

Device Management Code: •••••••

Confirm Management Code: •••••••

Data Destruction: □

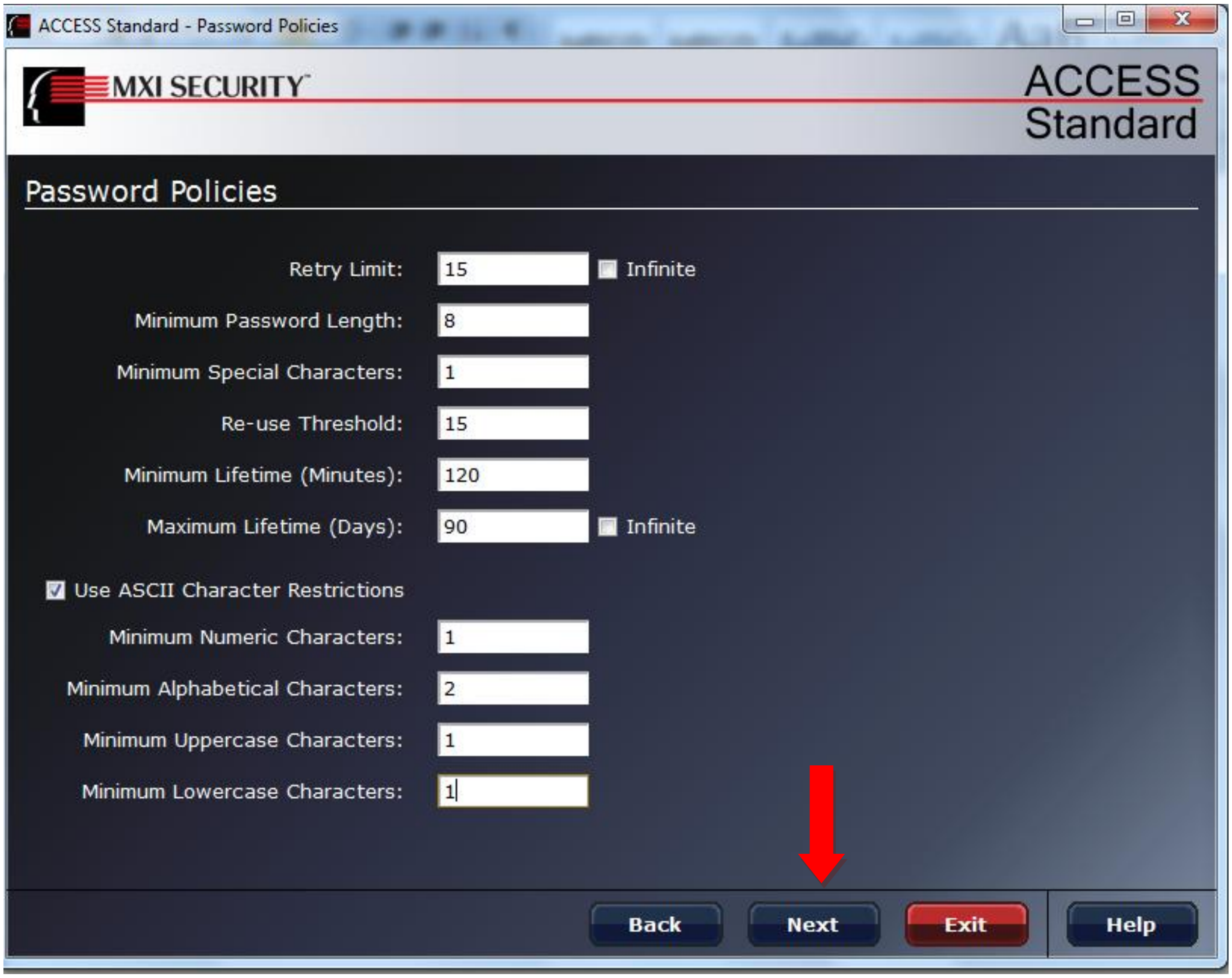
Disable Administrator's Account: □

Hide Usernames Before Authentication: □

[Next Page]

[1] This is the code word needed to reset the device (erases all data and security policies) for reuse.

11. Device Personalization Step 3: Password Policies—Do not deviate from these settings
    a. Retry Limit = 15
    b. Maximum Password Length = 8
    c. Minimum Special Characters = 1
    d. Re-use Threshold = 15
    e. Minimum Lifetime = 120
    f. Maximum Lifetime = 90
    g. Minimum Numeric Characters = 1
    h. Minimum Alphabetical Characters = 2
    i. Minimum Uppercase Characters = 1
    j. Minimum Lowercase Characters = 1
    k. Click **Next**



Password Policies

Retry Limit: 15 □ Infinite

Minimum Password Length: 8

Minimum Special Characters: 1

Re-use Threshold: 15

Minimum Lifetime (Minutes): 120

Maximum Lifetime (Days): 90 □ Infinite

☑ Use ASCII Character Restrictions

Minimum Numeric Characters: 1

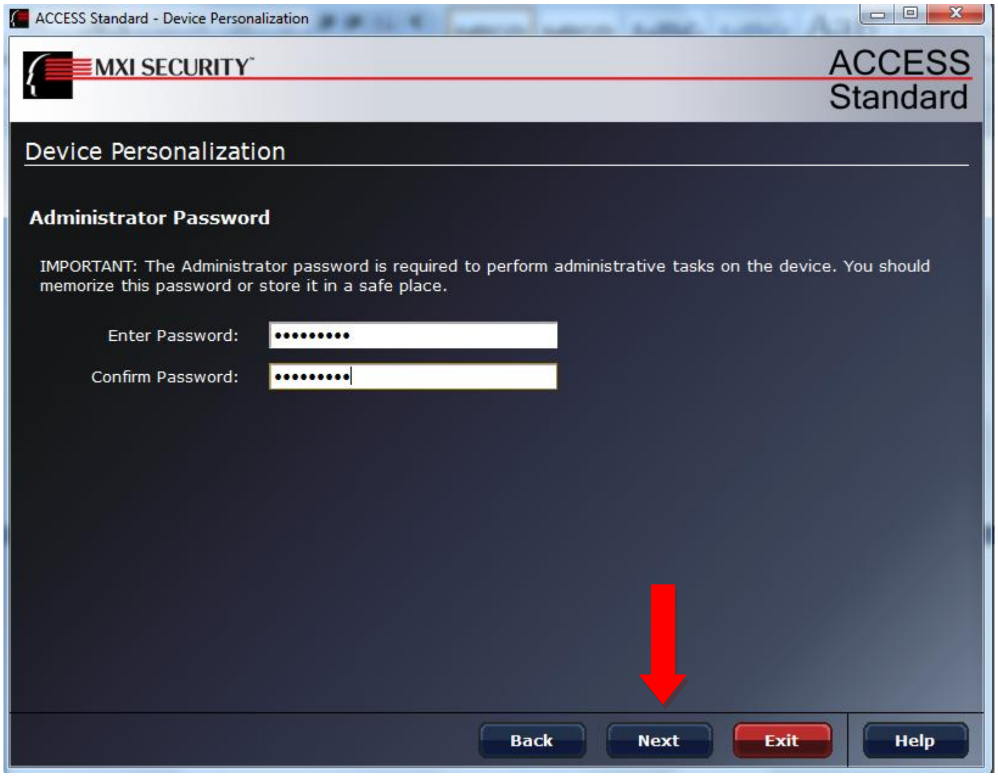
Minimum Alphabetical Characters: 2

Minimum Uppercase Characters: 1

Minimum Lowercase Characters: 1

These settings establish the password policies and closely mirror those required by the FSSA Privacy Compliance Policy. The settings force a complex password and force the user to reset their password every 90 days. A complex, secret password is the only defense against someone hacking into the device and getting to the encrypted data should the device be lost or stolen.

12. Device Personalization Step 4: Enter and Confirm Administrator Password
    a. This is your (the MXI Device Administrator) password, which you will need to reset the user's password should they forget it.
    b. **Enter** a complex password—the same password policy (above) applies
    c. **Re-enter** the password in the Confirm Password box
    d. You may use the same administrator password for all MXI Devices you issue
    e. Keep the administrator password secret
    f. Click **Next** to continue



Device Personalization

Administrator Password

IMPORTANT: The Administrator password is required to perform administrative tasks on the device. You should memorize this password or store it in a safe place.

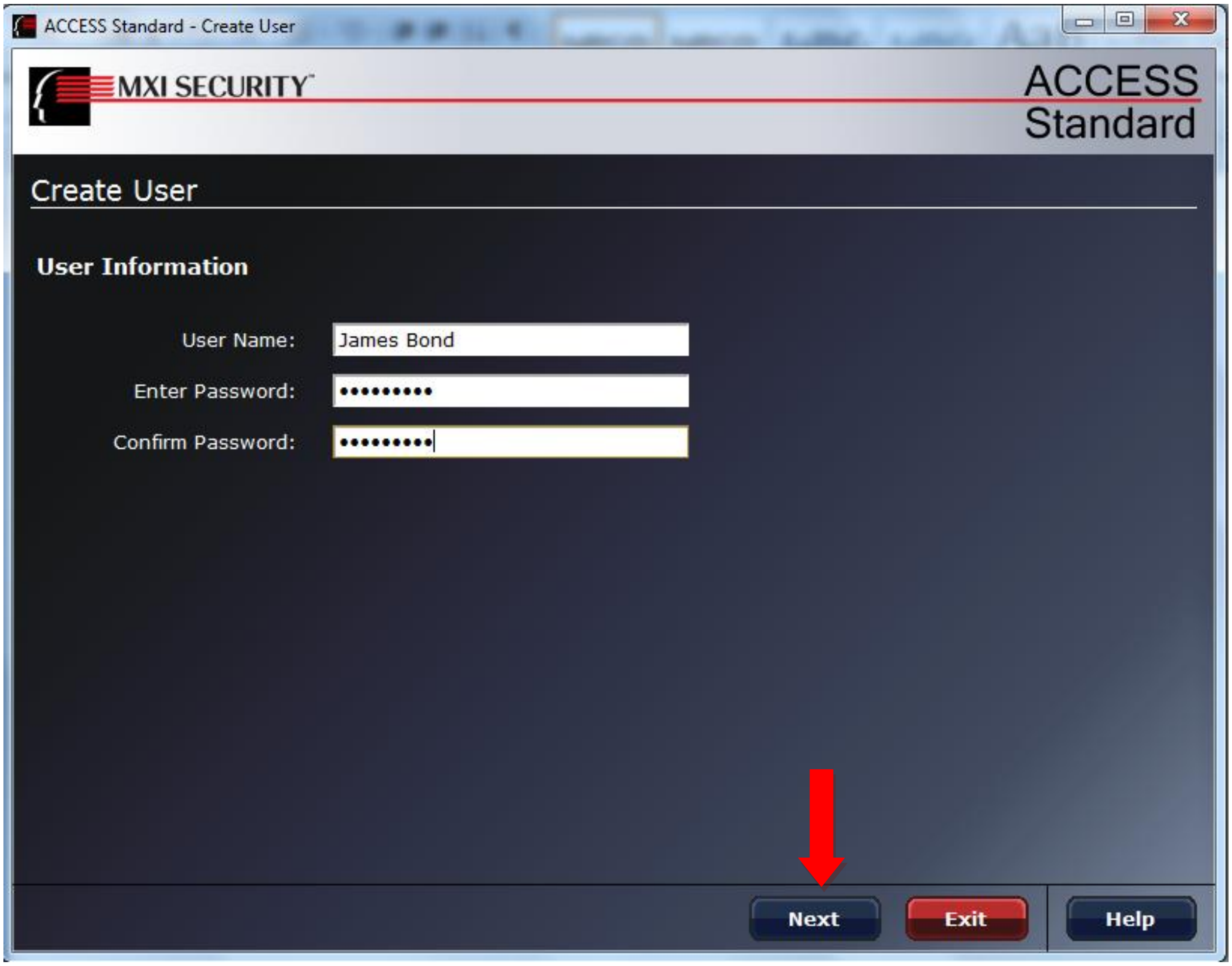
Enter Password: •••••••••

Confirm Password: •••••••••

Note: while it is important to keep the Administrator Password secret, the program area MXI Device Administrator should provide their manager with a copy of the password (to be kept safe and secure) so that the manager may act in the stead of the Administrator in the Administrator's absence.

[Next Page]

13. Device Personalization Step 5: Create User
    a. For each user you are providing a MXI Device
    b. **Enter** their user name: this should be either their first and last name, or their State network User ID
    c. **Enter** an initial password for the user—a complex password is required (see above)
    d. **Confirm** the initial password for the user by re-entering it in the Confirm Password box
    e. You will provide this password to the user when you give them the MXI Device
        i. They are instructed to change this initial password on first use (see MXI USB Drive User Instructions)
        ii. Because there is no data yet on the device, you may use the same initial password for all users
    f. Click **Next**



Create User

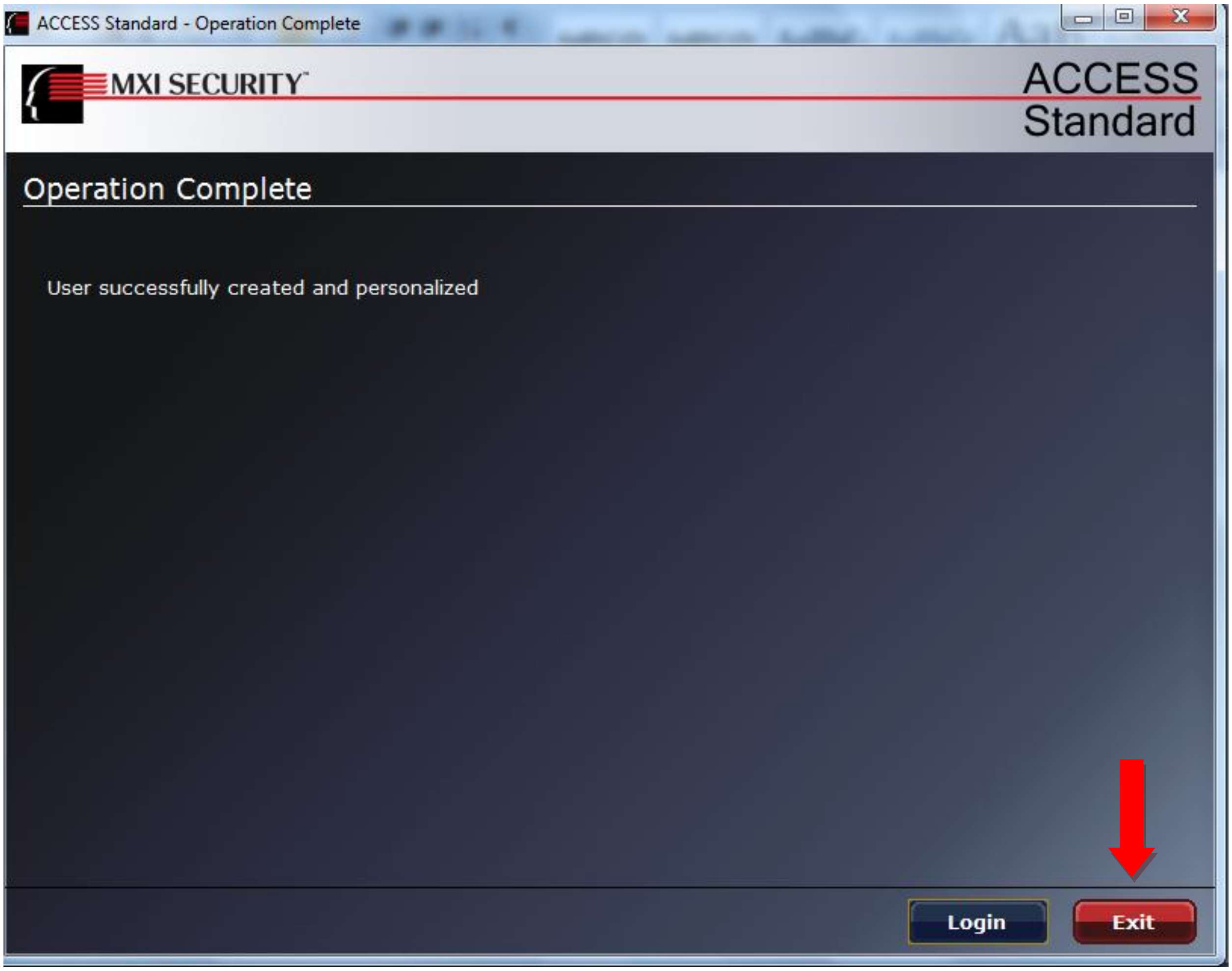
User Information

User Name: James Bond

Enter Password: ••••••••••

Confirm Password: ••••••••••

14. Device Personalization Step 6: Operation Complete
    a. The following screen should appear; the light on the device should be red indicating the device is now secured and locked
    b. Click **Exit**



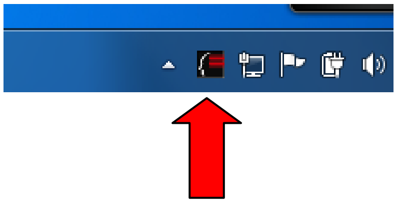
ACCESS Standard - Operation Complete

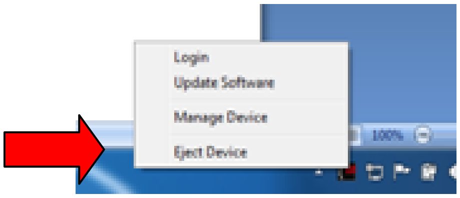
Operation Complete

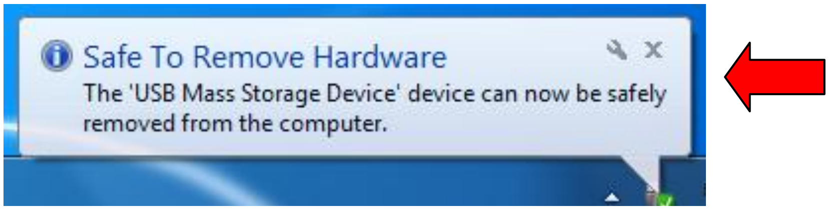
User successfully created and personalized

[Next Page]

15. **Right** click on the MXI ACCESS icon in the system tray (lower right of the screen, and click **Eject Device.** **Wait** until you receive the Safe to Remove Hardware notice before you remove the device.







Safe To Remove Hardware

The 'USB Mass Storage Device' device can now be safely removed from the computer.

16. Complete the MXI Device inventory sheet for the device:
    a. Division/Program Area
    b. User Name
    c. User Location
    d. Device Serial Number
    e. Date Issued