CSCU

Connecticut State
Colleges & Universities

Drive Encryption End User Guide

(Revision Date: 07/09/2020)

Table of Contents

Introduction

McAfee Drive Encryption delivers encryption that protects data from unauthorized access, loss, and exposure using Preboot authentication (PBA) and a powerful encryption engine. It is designed to make all data on a system drive unintelligible to unauthorized persons and reinforce organizational security measures in accordance with the CSCU Security Policy.

To access data on a laptop computer, you must first be enrolled as a Drive Encryption user by an IT Administrator and granted access to the laptop. Upon initial login, you should be guided by a member of your college IT helpdesk following the First Time Login procedure. After completing the procedure, your Drive Encryption Logon account will be synchronized with the Windows account and your netID and password can be used to authenticate at the PBA screen. It is important to keep the encryption password consistent with the Windows password for both accounts to remain synched. When it is time to change your Windows password, follow the procedure documented in this guide.

Intended Audience

The intended audience for this procedure is:

- CCC Employees
- CSCU Employees

Procedure

Changing Your Windows Password and Drive Encryption Password

When it is time to change your netID or Windows password, it is very important to perform the change from the assigned laptop. Doing this will allow the Drive Encryption password to remain synchronized with the Windows password. Synchronized passwords allow Drive Encryption to perform Single Sign-On and login to Windows automatically. If you change your Windows password from another location, such as your desktop, your Windows account, and your Drive Encryption Logon will no longer be synchronized.

To change your Windows password:

1. Always change your password prior to the expiration date to avoid login issues. When you are ready to make the change, be sure your laptop is connected to the ConnSCU network over Wifi or wired connection.

2. Login to the encrypted laptop with the netID and password. If the encryption password is synchronized, Windows will perform SSO and automatically sign you in.

3. Once the desktop is loaded, press **Ctrl + Alt + Delete**, then click **Change Password.**

4. Enter your current password and then create a new password. Press **Ok** to submit the change.

   NOTE: If you see the error: "**Unable to change the password on this account due to the following error: There are currently no logon servers available.**" It means you are not connected to the ConnSCU network. You cannot change your NetID password without being connected to the ConnSCU network. Press **OK** to continue. You will need to connect to the ConnSCU network before you can change your Windows password.

5. Now that your Windows password is changed from the encrypted device, allow 60 minutes to elapse and then reboot the laptop.

6. At the Drive Encryption Login screen, enter your username and when prompted for password, enter your new Windows password.

7. Single Sign-On will work on the next reboot.

- It is extremely important to safeguard your password and not disclose it to anyone or write it down. If your password is compromised, Drive Encryption no longer protects your confidentiality.

- If you did not change your netID password from the encrypted device, you will need to manually change it for Drive Encryption on the laptop at login. Submit a ticket to the Service Desk for further assistance at ServiceDesk@ct.edu.
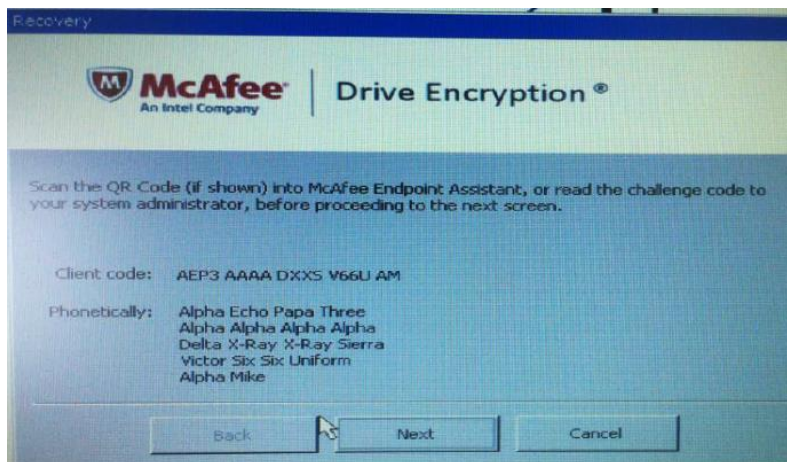
Recovering Your Drive Encryption Logon Password

Refer to these instructions when you are unable to login to Drive Encryption with an old or a new password.

If you continue to encounter problems logging into the Drive Encryption window, you will need to have your Drive Encryption Logon password recovered.

1. Boot the machine up to the Drive Encryption Screen, click on **Options**, **Recovery**:
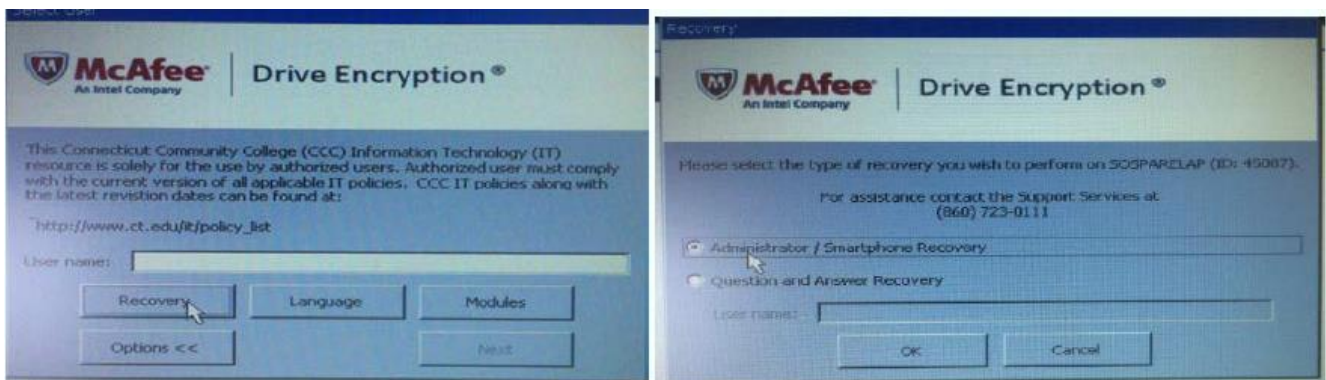
2. Select **Administrator/Smartphone Recovery**, you will see a Recovery Window as shown below:
3. A **Challenge code** will be displayed and phonetically represented to help avoid mistakes when reading the code over the phone.


4. Call your local college helpdesk and report that you need your Drive Encryption Logon password recovered. The technician will work with you to complete the remaining steps:

1) Read the code to the helpdesk person
2) Click **Next**.
3) They will read two lines of response code back to you that you need to enter Line1, hit **Enter** and then complete Line 2.
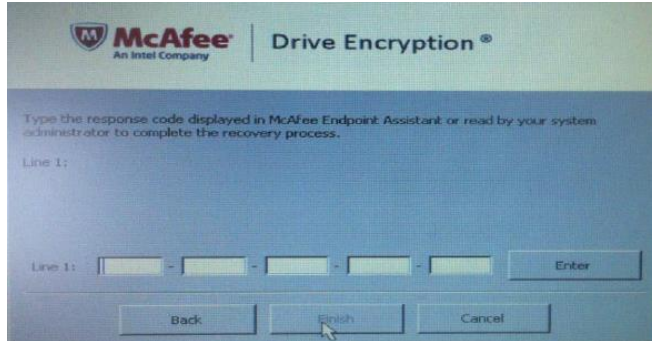
4) Click **Finish**

5. if successful, you will be prompted with a change password dialog box. Enter your current Windows password and then click **OK.**
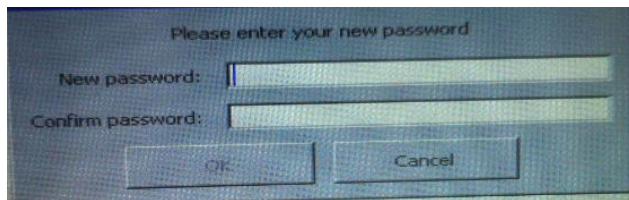
6. After resetting the password, the Drive Encryption screen will load. Enter the new password to login.

Release History

☐   05/16/2014 Initial Release