CSCU

Connecticut State Colleges & Universities

Drive Encryption Procedure

End User Documentation: First Time Login

(Revision Date: 7/10/2020)

Table of Contents

Introduction

ConnSCU encrypted laptops contain an authorized user's list that permits users to login to Drive Encryption. If you are not a member of the authorized user's list, you will not be able to login.

As you are already familiar with, to login to the ConnSCU network, you use your NetID (ie: 00000123@commnet.edu). The NetID also refers to your Windows account. If you are going to be logging into an encrypted laptop, you will now need a 2nd type of account, called the Drive Encryption Logon account.

The good news is the Drive Encryption Logon username and your Windows username will be the same. Therefore, if you login to your desktop PC as 00000123@commnet.edu, you will also be logging into an encrypted laptop as 00000123@commnet.edu.

The Windows account and the Drive Encryption account are synchronized the first time you login to an encrypted laptop. When the password for your Drive Encryption Logon matches the password for your Windows account, a single logon attempt is all that is needed to authenticate pass Drive Encryption and the Windows logon. This process is known as a Single Sign-On authentication.

Once you have an account to access encrypted laptops, any updates, or changes to your NetID password must reflect the Drive Encryption Logon password. To keep your NetID credentials synced with the Drive Encryption Logon, be sure to make password changes from the encrypted laptop. Doing this will ensure that both account passwords are the same. If you change your Windows password from another location other than the laptop, such as your desktop, your Windows account and your Drive Encryption Logon will not remain synced.

The first time you login to an encrypted laptop, you will set the encryption password to match your Windows password. The following procedure ONLY applies the first time you login to any encrypted laptop and once set, does not need to be repeated, even if you are logging into other encrypted laptops.

This guide will walk you through the initial logon procedure.

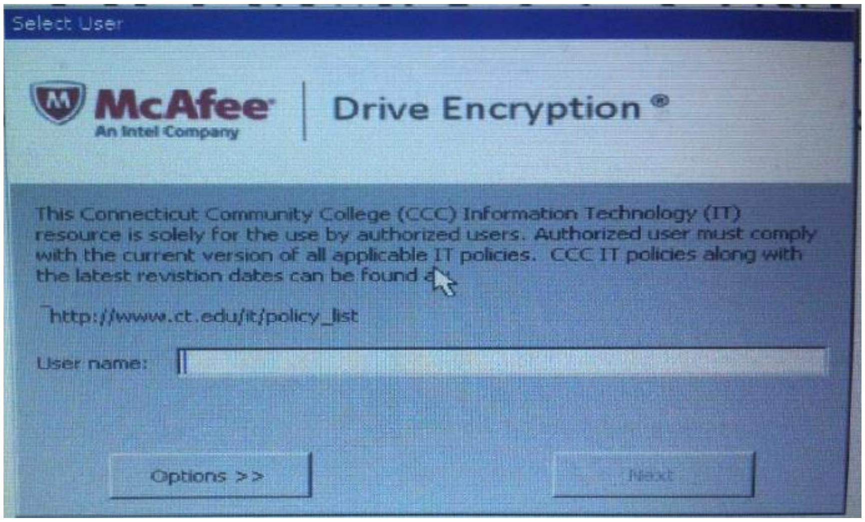
Intended Audience

The intended audience for this procedure is:

- Community College Employees
- System Office Employees

Procedure

1. Power on the laptop and connect to the ConnSCU network.
   The very first screen you will see is the McAfee Drive Encryption logon:

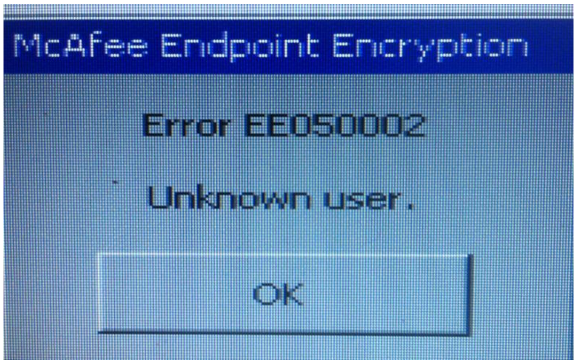


This Connecticut Community College (CCC) Information Technology (IT) resource is solely for the use by authorized users. Authorized user must comply with the current version of all applicable IT policies. CCC IT policies along with the latest revistion dates can be found a

http://www.ct.edu/it/policy_list

User name:

2. Enter your netID for User name and click **Next**.
   - If you receive the following error and you have not mistyped your User name, make sure that the Drive Encryption Administrator verifies your Account has access to login to the device.

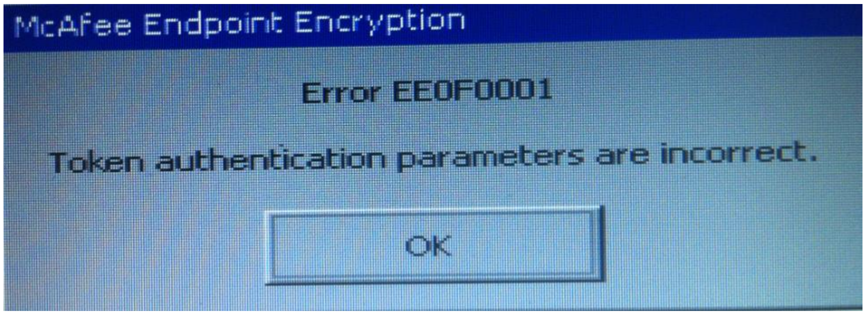


McAfee Endpoint Encryption

Error EE050002

Unknown user.

3. The Drive Encryption Administrator should have provided you with the default initial password. Enter the password and click Ok. if you mistyped it, you would get the following error.

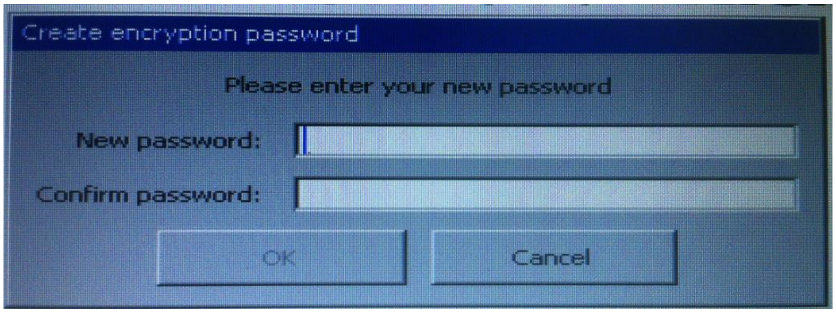


McAfee Endpoint Encryption

Error EE0F0001

Token authentication parameters are incorrect.

4. Once you have successfully logged in with the default password, you will be asked to set a new password. Make the password your current Windows account password to sync the Drive Encryption Logon with the Windows account.



Create encryption password

Please enter your new password

New password:

Confirm password:

Enter your current Windows account password, confirm it, and then press **OK.**

5. Once you have successfully set your Drive Encryption Logon password, the laptop will be decrypted and load the Operating System. Login to Windows with your NetID and password.
6. After logging in, the Drive Encryption Administrator will perform a Wakeup Agent call from the ePO server to synchronize your password with the encryption server for future logins.

7. Reboot the machine and login once more to verify your Drive Encryption Logon and Windows account passwords are synchronized. You will notice that Single Sign-On now works as expected and you no longer have to login to Windows separately.

Release History

□	05/16/2014	Initial Release
□	7/10/2020	Update Drive Encryption 7.2.9