

End User Documentation: First Time Login

(Revision Date: 4/11/2013)

Table of Contents

Introduction	1
Intended Audience.....	2
Procedure.....	2
Release History	4

Introduction

ConnSCU encrypted laptops contain an authorized user list. In order to login to an encrypted laptop, you need to be on that list; otherwise you will not be able to login.

As you are already familiar with, to login to the CCC network, you use your Windows Account (ie.00000123@commnet.edu or doej@ct.edu). If you are going to be logging into an encrypted laptop, you will now need a 2nd type of account, called your Endpoint Encryption Logon.

The good news is the Endpoint Encryption Logon and your Windows username will be the same. So if you log into your desktop as 00000123@commnet.edu or doej@ct.edu , you will also be logging into an encrypted laptop as 00000123@commnet.edu or doej@ct.edu.

These two logins need to be synced the first time you login to an encrypted laptop so that your password for your Windows account is the same as the password the Endpoint Encryption Logon. This process is known as single sign-on.

Once you have an account for logging onto encrypted laptops, in order to keep your NetID username synced with your Endpoint Encryption Logon, you need to make sure that when you change your NetID password, that you perform the password change from the encrypted laptop. This will keep both passwords the same. If you change your Windows password from another location, such as your desktop, your Windows account and your Endpoint Encryption Logon will not be synced anymore.

The first time you login to an encrypted laptop, your accounts need to be initially synced. The following procedure ONLY applies the first time you login to any encrypted laptop and once set, does not need to be done again even if you are logging into other encrypted laptops.

This procedure will walk you through that procedure.

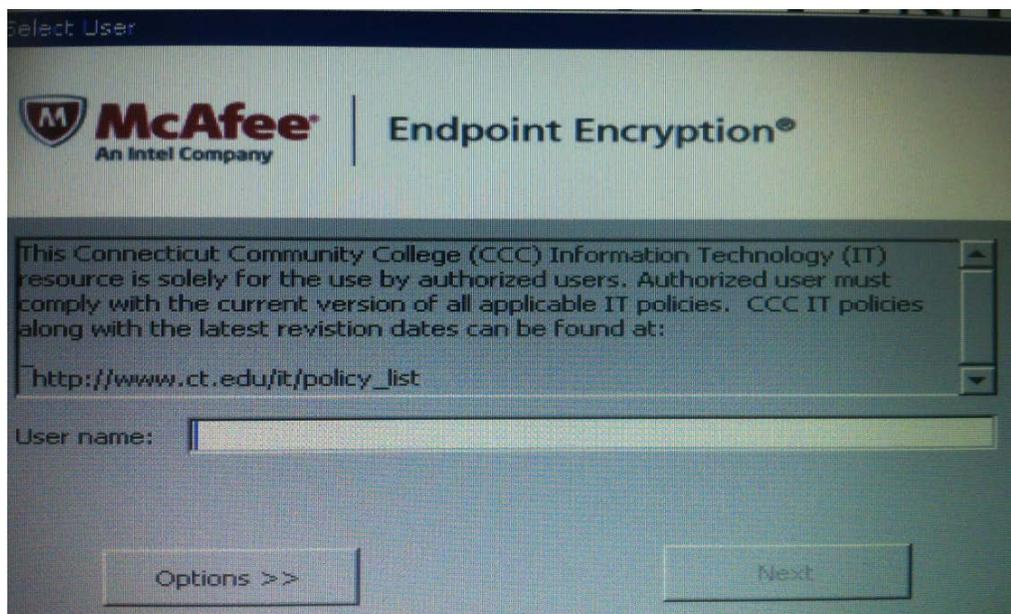
Intended Audience

The intended audience for this procedure is:

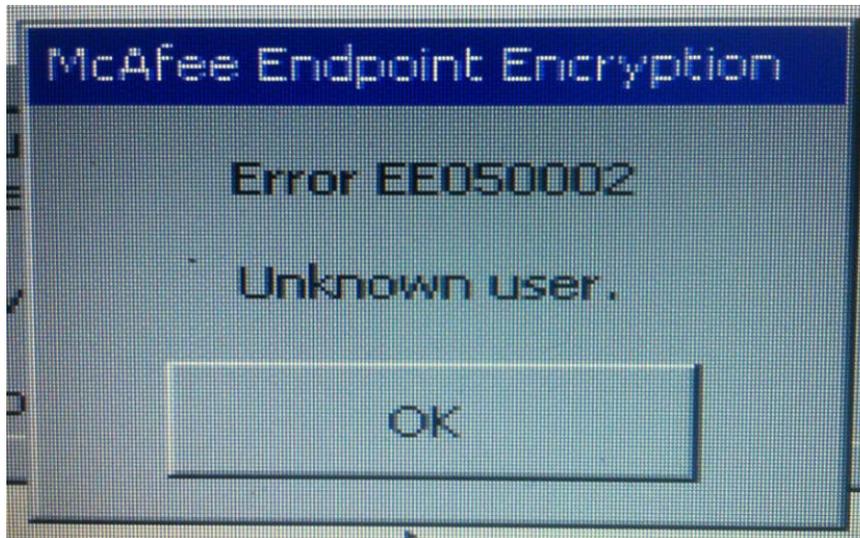
- Community College Employees
- BOR Staff

Procedure

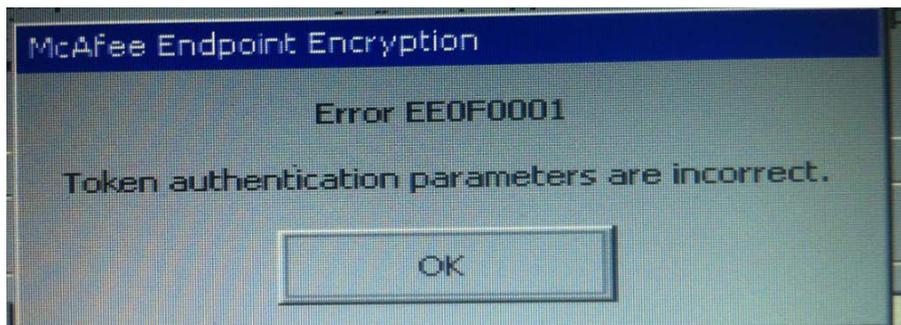
1. Connect the machine to the CCC network and power on the laptop. The very first thing you will see is the McAfee Endpoint Encryption logon screen:



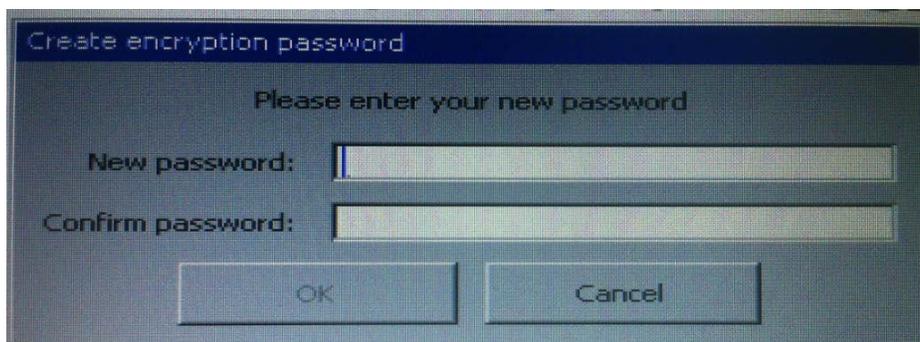
2. This is your Endpoint Encryption Logon which has the same username as your Windows account. Enter your Account name. If you receive the following error and you haven't mistyped your Username, make sure that the Endpoint Encryption Administrator verifies that your Account has access to log into the device.



3. Type in your default password, if you mistyped it, you will get the following error



Once you've successfully logged in with the default password, you will then be forced to change your password. You are setting your Endpoint Encryption Logon password and want to set it to be the same password as your current Windows account password. This will sync the two passwords. Enter your current Windows account password and confirm it, then press **OK**:



4. Once you've successfully set your Endpoint Encryption Logon password, it will decrypt the drive and Windows will then start and prompt you to login. You then need to log into Windows with your Windows account username and password as you normally do.

5. After Windows boots, the Endpoint Encryption Administrator has to do a Wakeup Agent call from the ePO server to synchronize the password change with the encryption server for future logins.
6. Reboot the machine after synchronizing and login once more to verify your Endpoint Encryption Logon and your 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

- 4/11/2013 Initial Release