

# McAfee Endpoint Encryption (SafeBoot) User Documentation

---

## TABLE OF CONTENTS

*Press the CTRL key while clicking on topic to go straight to the topic in this document.*

I. Introduction .....	1
II. Installation Process Overview .....	1
III. Checking for a Valid Current Backup .....	1
IV. Encryption Status .....	2
V. Notes About Your Windows and Endpoint Encryption Passwords .....	2
VI. Boot-Up/Login Process .....	3
VIII. Changing Your Password .....	4
IX. Shutdown Process .....	4
X. Notes for Encryption .....	5
XI. Forgotten Password .....	6
XII. Frequently Asked Questions (FAQs) .....	8

## I. Introduction

---

Congratulations! You have been selected to participate in the full disk encryption program. ***The goal of this project is to protect sensitive data that is stored on the University of Toledo's laptops and workstations.*** McAfee Endpoint Encryption has been chosen as our encryption tool, which will encrypt all of the data on the internal hard drive of your machine while having minimal disruption to your everyday work.

## II. Installation Process Overview

---

Details for the following process are included in the subsequent documentation:

- Request for encryption software
- Software installation scheduled for user
- Email sent to user confirming request and instructing them to verify backups
- User verifies backups (or resolves issues with Help Desk)
- Tech is deployed to machine to complete the Installation
- Laptop encryption begins and should be completed within 4-5 hours
  - This takes place in the background, allowing normal use of laptop

## III. Checking for a Valid Current Backup

---

Prior to initiating the installation, please ***ensure that you have backed up the data on your machine to either the network or to removable media, such as a thumbdrive.*** Should your machine become inaccessible during the installation process, the backup will be used for the recovery of your data. The same technology that protects your laptop may also make it difficult to recover this data should the install process not complete successfully (usually this is due to failed hardware). This scenario is rare, but it is important that we prepare for it.

This is a good time to remove any data from your machine that does not have an immediate business need.

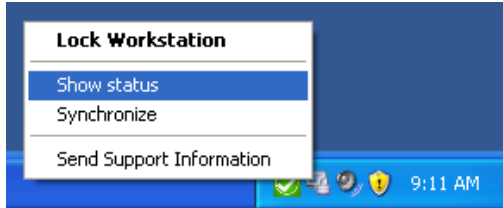
**If you have questions about the backing up your data, please contact your local IT personnel or the Help Desk (x2400) for assistance.**

---

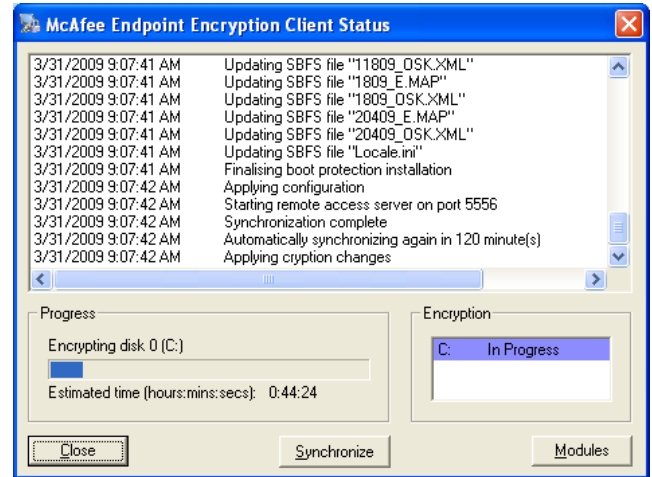
# McAfee Endpoint Encryption (SafeBoot) User Documentation

## IV. Encryption Status

1. After the installation of Endpoint Encryption, you can monitor the status of the encryption process by right-clicking on the Endpoint Encryption icon in the System Tray and choosing "Show status."



2. Under the "Encryption" box, the status will change from "In Progress" to "Encrypted" when the encryption is complete.
  - a. At that time, all data on your laptop/workstation will be fully encrypted.
  - b. Any new files copied or saved to your C:\ drive will be encrypted as well.



## V. Notes About Your Windows and Endpoint Encryption Passwords

1. The McAfee Endpoint Encryption product will synchronize your pre-boot password to your UTAD (Windows) password. This means that you will only be required to remember one password and will be required to enter it only once upon bootup.
2. It is imperative that you utilize the [myutaccount](#) website to change your password. This will ensure that any password changes that are done in Windows will be propagated to the Endpoint Encryption product so that your passwords stay in synch. See the section [Changing Your Password](#) for instructions on changing your password.

# McAfee Endpoint Encryption (SafeBoot) User Documentation

## VI. Boot-Up/Login Process

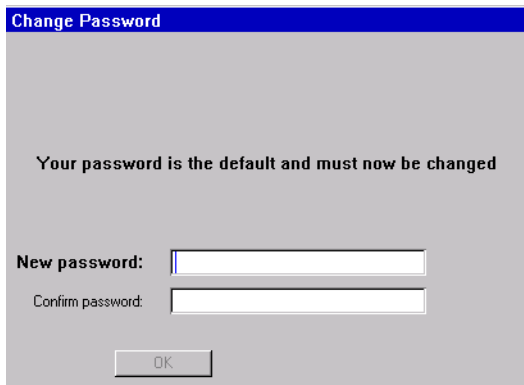
1. Now that encryption is installed, you will see a screen similar to the following every time you boot. This is known as the “pre-boot screen.”



2. Enter your username (UTAD/ NetworkID) and password and press “OK.”

**If this is the first time you are booting, and you have not previously signed on to Endpoint Encryption, you will need to enter the default password provided by the tech that is installing the product.**

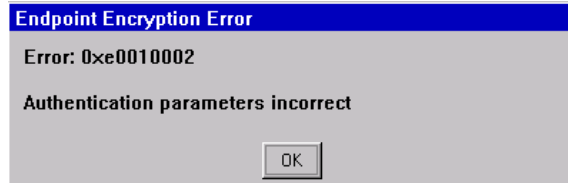
After entering this default password, you will be prompted to change your pre-boot password. At this point you will want to enter your Windows credentials so that your passwords are in synch.



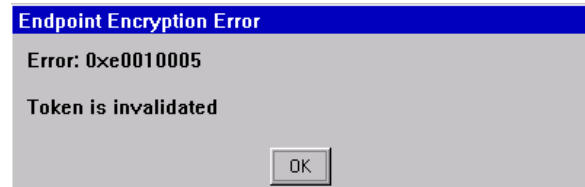
3. After successfully authenticating to this pre-boot screen, your

machine will then continue booting as normal. Since your passwords have been synched, your Windows password will be automatically entered into the Windows logon window and you will be presented to your desktop, just as if you had entered these credentials yourself.

If you enter the wrong credentials at the pre-boot screen, you will get an error message stating that “Authentication parameters incorrect.” If you need assistance in resetting your password, see the section on [Forgotten Password](#).



4. If you do not enter your password correctly after 10 attempts, your ID will be disabled and you will see the following screen. At this point, you will be *required* to call your local support or the Help Desk for assistance in resetting your password.



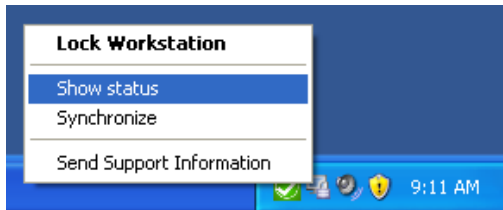
See [Forgotten Password](#) section below to re-enable your ID.

5. After the initial installation, you will be required to enter your credentials once more through the normal sign-on process. This ensures your pre-boot password gets synched with your Windows password.
  - a. This ensures your pre-boot password gets synched with your Windows password.
  - b. On subsequent reboots, the info entered on the McAfee Endpoint Encryption pre-boot screen will be automatically passed and verified behind the scenes to Windows.
6. Whenever you change your Windows password, it will be synched up with the pre-boot password. Use this new password for your pre-boot credentials on subsequent reboots.

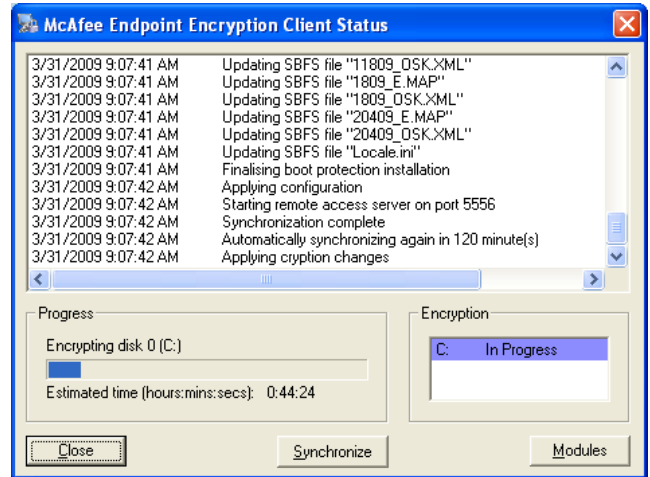
# McAfee Endpoint Encryption (SafeBoot) User Documentation

## VIII. Changing Your Password

1. The McAfee Endpoint Encryption product will synchronize your pre-boot password to your UTAD (Windows) password.
2. It is imperative that you utilize the [myutaccount](#) website to change your password. This will ensure that any password changes that are done in Windows will be propagated to the Endpoint Encryption product so that your passwords stay in synch. Be sure to log off and then back on to Windows after changing your password for it to take effect.
3. After changing your password on [myutaccount](#), you will want to then synchronize this password change so that your machine will receive this updated Endpoint Encryption password. Click on the Endpoint Encryption icon in the System Tray and choose "Show Status."



4. Now choose the "Synchronize" button.



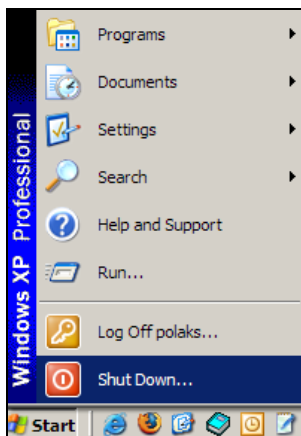
5. You should then see the synchronization take place in the status window. After the synchronization competes (several seconds), your Endpoint Encryption password will be synced with your Windows password.
6. Be aware that your machine will automatically synch every 2 hours without user intervention (provided that it is on and connected to the UT network), so if you have forgotten to perform the synchronization step, your machine will eventually get updated automatically with this password change anyway.
7. Note that if your passwords do become out of synch, you can manually change your Endpoint Encryption password to your Windows password. See the FAQ [here](#) on how to do this.

## IX. Shutdown Process

**IMPORTANT: Always shut down your machine completely--DO NOT put your machine in Standby mode.**

Bringing your machine out of "Standby" will NOT require you to authenticate to the pre-boot screen. This poses a security risk to the data on your machine by leaving the computer in an unsecured state when not in use. Where practical, always do a complete shutdown of your machine at the end of the day or when traveling with your laptop.

1. To shutdown completely, select **Start > Shut Down**.



2. From the pull-down list, select **Shut down**.



# McAfee Endpoint Encryption (SafeBoot) User Documentation

---

## X. Notes for Encryption

---

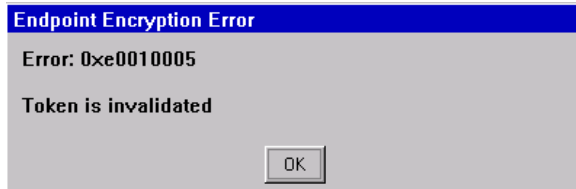
- \* You can work on your machine while the initial encryption is executing—it will continue to run seamlessly in the background.
- \* You can also safely shut down your machine while the initial encryption is running, although it is recommended that you leave your machine running if possible until the encryption completes.
- \* Your entire hard disk will be encrypted. Any file that is moved from your machine to a network share, email, or another machine will **NOT** be encrypted. This encryption product will only protect your local machine. Be aware of the encryption implications when transferring files to another medium.
- \* When shutting your machine down for the day or when traveling with your laptop, **do not place the machine in standby mode.** You should shut down completely. This will require you to re-authenticate to the McAfee Endpoint Encryption product when you restart it. Putting your machine in “standby” mode will not require you to re-authenticate with Endpoint Encryption, and can put your data at risk.
- \* Be extra diligent in remembering your password. The process that makes it difficult for an unauthorized person to decrypt your hard drive also makes it (somewhat) cumbersome to recover your password.
- \* The best method for protecting data is to not put it on your machine in the first place. Only data that has an immediate business need, especially that of a confidential/sensitive nature, should be stored on your machine. It is best that you do not keep any confidential/sensitive data on your machine if at all possible. Defense in depth is the best way to protect your data, and that starts with not keeping unneeded data on your laptop in the first place. Where practical, the first choice for any data storage should be on a network drive (either H: or Z: drives).

# McAfee Endpoint Encryption (SafeBoot) User Documentation

## XI. Forgotten Password

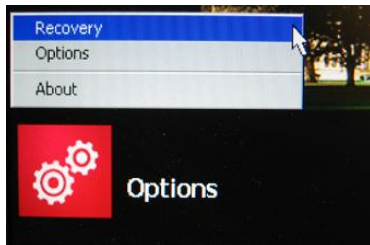
The same process that makes it difficult for an outsider to decrypt your machine also makes it somewhat difficult to recover your password if you forget it. Therefore, it is highly recommended that you make a concerted effort to remember your password. If you have forgotten your password, you can use the following method to unlock your machine. Note that this method also applies if your ID has become disabled due to too many password-guessing attempts.

1. If you have attempted to log on unsuccessfully 10 times, your ID will be disabled. You will see the following dialog box if your ID is disabled:



Please note this when calling the Help Desk.

2. At bootup, close (cancel) all dialog boxes, click the "Options" link on the bottom left of the screen, and then choose "Recovery."



3. The recovery screen will now be displayed. Select the "User recovery" radio button and enter your Network ID.



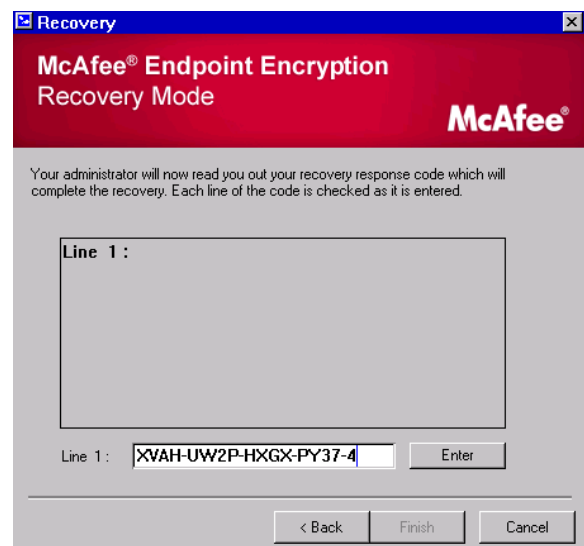
4. Select "Next." You will now want to call your local support or

the Help Desk (x2400) for assistance and inform them that you need your McAfee Endpoint Encryption (SafeBoot) password reset. If your ID has become disabled (see [Step 1](#)), make sure that you convey this to the Help Desk.

5. Give the Help Desk technician the 16-character "Client code" (challenge) that should now be displayed on the screen.



6. You will then want to click "Next." The Help Desk will provide you with a 17-character code (response) that you should now enter into "Line 1" on the Recovery screen. (Note that for a disabled user, this will be a 25-character code.)



## McAfee Endpoint Encryption (SafeBoot) User Documentation

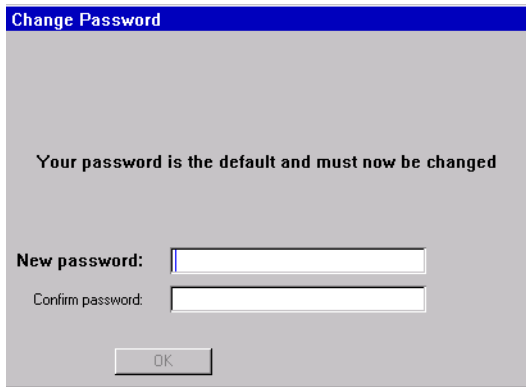
---

7. After entering all of the characters, choose "Enter" and then "Finish."
8. If you enter the numbers *incorrectly*, you will get the following dialog box:



If you get this screen, click the "OK" button to go back to [Step 6](#) and re-enter the characters.

9. If you successfully enter the characters, you will be prompted for a new password.



10. Once you enter your new password correctly, you will get the following confirmation screen:



11. Select "OK." You will then be placed back into the pre-boot screen. Select "Password Only Token," enter your ID and your new password, and select "OK." You should then be booted into Windows as normal.
  12. You will now want to open a browser and navigate to the [myutaccount](#) website to reset your Windows password. You can enter the same password at this website that you used in [Step 9](#).
  13. If you are NOT connected to the UT network, your Windows credentials may still work, but you will **want to connect to the UT network as soon as practical so that you can reset your Windows password.**
-

# McAfee Endpoint Encryption (SafeBoot) User Documentation

---

## XII. Frequently Asked Questions (FAQs)

---

Q: Do I have to remember a separate password for Endpoint Encryption?

A: No. Your Endpoint Encryption and Windows passwords will synch whenever you change your Windows password. You will be required to provide this password when your machine boots. It is imperative that you use the [myutaccount](#) website to change your password, as this will ensure that your Endpoint Encryption password gets updated as well, regardless of the machine that you utilize to change your password on. See [Changing Your Password](#).

Q: Since my passwords are synched, do I have to enter the password a second time in order to log into Windows?

A: By default, no. Your machine is set up to utilize a functionality called single sign-on (SSO), which will automatically provide your credentials to Windows to log you on (after you provide them at pre-boot). If you log in from home using a different ID than your regular ID (due to slowness of logon/logoff scripts) and wish to have the functionality of SSO removed, please contact Security Services.

Q: How do I log on as a different Windows user than my Endpoint Encryption user?

A: You must first log off of Windows. You can then log back on as a different user through the Windows logon screen. If you are using Vista, be sure to select the "UTAD" credential provider box (and not the "Endpoint Encryption" one).

Q: My passwords are not synched, but I know both my Endpoint Encryption and Windows password.

A: There are some instances where your passwords will not synch properly between Endpoint Encryption and Windows. If you currently can log onto Endpoint Encryption, you can manually set this password to your Windows password by following the instructions below:

1. Enter your Endpoint Encryption credentials at pre-boot. Do **not** hit OK.
2. Check the box "Change password" and then press "OK."
3. You will be prompted to enter a new password. Enter your Windows password (twice), and then select OK."
4. Your Endpoint Encryption password should now be changed and synched with your Windows password.

Q: My password does not work on the pre-boot screen. What should I do?

A: If you have recently changed your Windows password, try entering your previous password. There are some instances where your Endpoint Encryption password could potentially become out of synch with your Windows password. If entering your old password works, you will want right-mouse click on the Endpoint Encryption icon in the System Tray, and select "Synchronize" after Windows completes its boot process. This will synchronize your Endpoint Encryption password with your Windows password. See the section [here](#) for synchronizing your machine to the Endpoint Encryption server. If this still does not work, it is recommended that you change your Windows password on the [myutaccount](#) web site and then re-synch your machine.

Q: My pre-boot password still does not work. Now what?

A: Call the Help Desk or your local support organization and follow the [Forgotten Password](#) instructions.

Q: Are files that I save on network shares encrypted as well?

A: No, only files on your local machine's hard drive are encrypted.

Q: Are files that I store on my thumbdrive/external hard drive encrypted?

A: No, only files on your local machine's hard drive are encrypted.

Q: If I send a file to a colleague in email, is it encrypted?

A: No, only files on your local machine's hard drive are encrypted. If you wish to encrypt email, see instructions located [here](#).

Q: Can I work on my machine while it is performing the initial encryption?

A: Yes. You may notice a *slight* decrease in performance while this process is executing, but this decreased performance will cease when the encryption has completed (usually 4-5 hours).

Q: Can I shut my machine down while it is encrypting?

A: Yes, but it is not recommended that you do so. If possible, you should wait for the encryption process to complete before shutting your machine down. If you have to shut it down, it will resume where it left off on the next startup.

Q: How do I know when my machine has finished encrypting my hard drive?

A: You can display the status of the hard drive encryption by looking at the [Encryption Status](#).

Q: How do I know if my machine is still encrypted?

A: You can display the status of the hard drive encryption by looking at the [Encryption Status](#).

Q: Is my machine protected if I put it into "Standby" mode?

A: Not completely. Since your machine will not require you to re-authenticate to Endpoint Encryption when bringing it out of Standby, it is recommended that you turn off your machine when travelling with it or when leaving for the day. See [Shutdown Process](#).

## McAfee Endpoint Encryption (SafeBoot) User Documentation

---

Q: Now that I have encryption on my machine, do I still have to be wary of the files that I store on it?

A: Yes. Encryption is only one piece of the security puzzle. It is best to have only data on your machine that has an immediate business need. It is recommended that any critical data be stored on a network drive/share. This will also address the need to back up this data. (Think of if your machine is lost or stolen—if your data is on a network share, you will still have access to it.)

Q: Why does the password recovery process seem so painful?

A: The same process that allows you to recover your password may also allow someone with nefarious intent to do so as well. We do not want to make it too easy for this to happen.

Q: Are Endpoint Encryption and SafeBoot separate products?

A: No. "SafeBoot" is now called "McAfee Endpoint Encryption," although you may still see some references to "SafeBoot."

Q: How come my keyboard/mouse doesn't work correctly in the pre-boot environment?

A: Certain keyboards and mice (especially the wireless versions) do not always work correctly in the pre-boot environment. Try rebooting your machine to see if it clears up any issues. If not, you will need to use a standard USB keyboard and/or mouse. Note that you can navigate in the pre-boot environment with just your keyboard (utilizing the TAB and ENTER keys), so you should not have to necessarily change out your mouse if it is not working.

Q: What type of encryption is used?

A: The entire contents of the hard drive are encrypted using the government standard AES-256 encryption algorithm. See description [here](#).