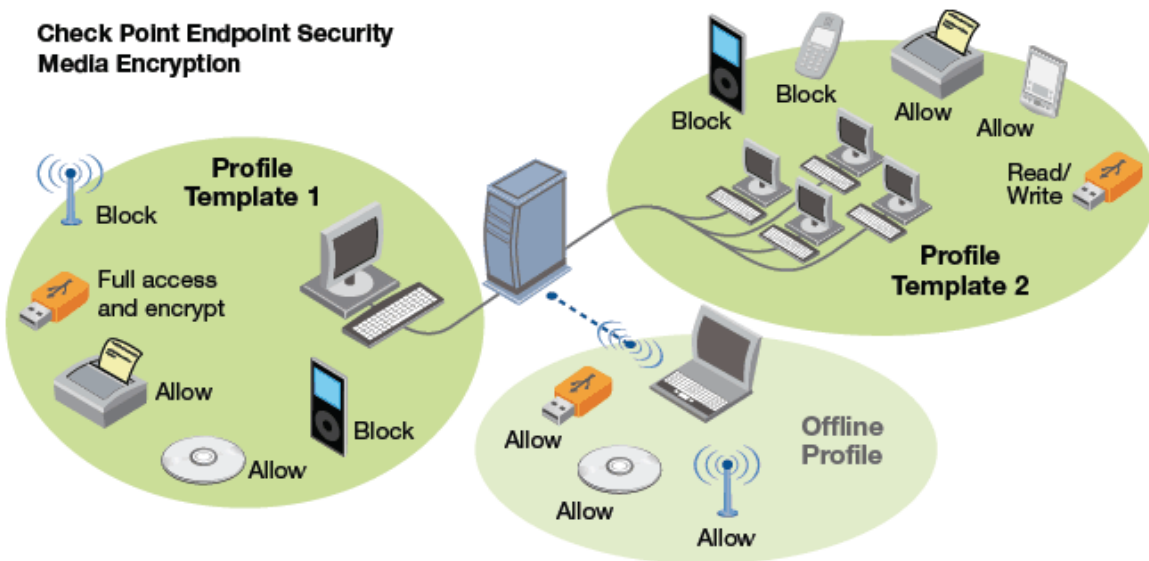


Media Device Encryption

The age of portable media has brought us a plethora of mobile media devices that allow information to be easily transported from place to place. Though portable media devices like CDs, flash drives, and SD cards offer incredible convenience to a workforce constantly on the move, they have birthed new lines of attack on your most sensitive information. Because a lost or stolen media device can mean losing information of paramount worth, it is important that steps be taken to safeguard your data.

Ferris will be distributing media device encryption software for faculty and staff laptops. The software will offer you the option to encrypt any media device when you plug it into your laptop. Opting to encrypt your media device will assure that it is always kept safe.



Frequently Asked Questions

What is MDE?

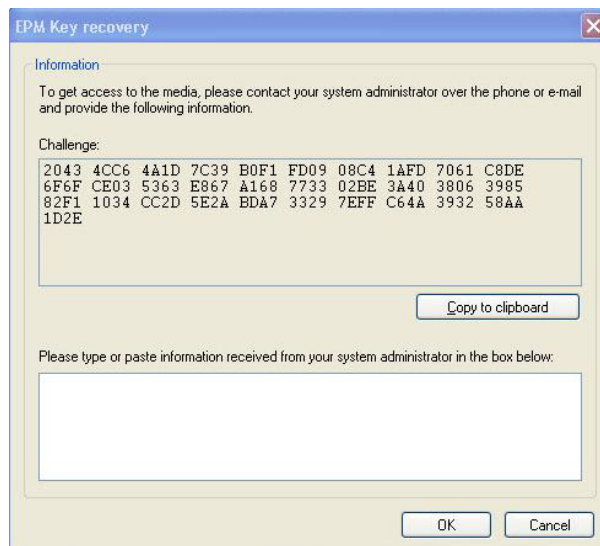
MDE stands for Media Disk Encryption. MDE is software that will encrypt your removable media devices so sensitive data cannot be accessed unless an authorized user name and matching password are supplied to the MDE software.

How do I reset the password on my flash drive if I forget it?

1. Plug in your media device and click **Cancel** on the log in screen to evoke the below prompt. Click the **Key recovery...** button.



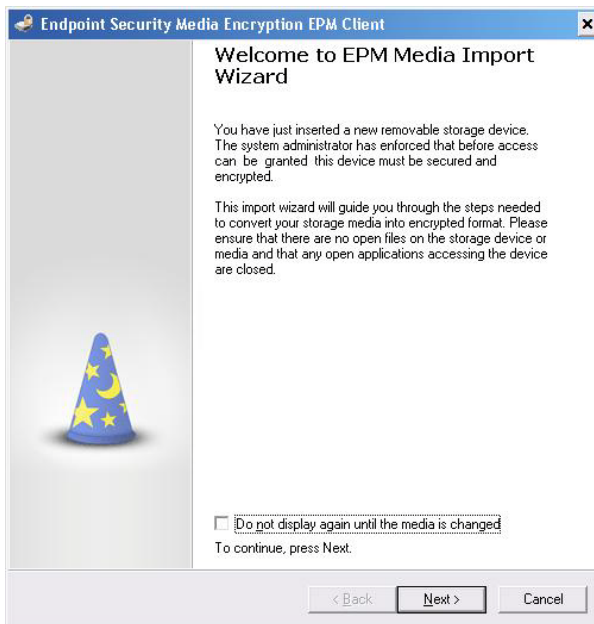
2. Next, the below screen will appear. Click **Copy to the clip board** to copy the challenge code so that you can paste it elsewhere. Call the Technology Assistance Center at 231-591-4822. A support representative will ask you to send him/her an email including the copied challenge code.



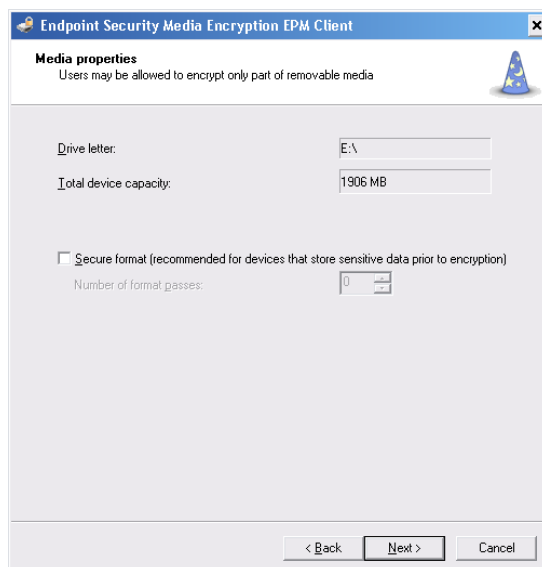
3. Your technology support representative will then give you a string of characters to enter into the empty box at the bottom of the prompt window. This will allow you to unlock your drive. Click **OK**.

How do I encrypt my flash drive after the MDE client is installed on my laptop?

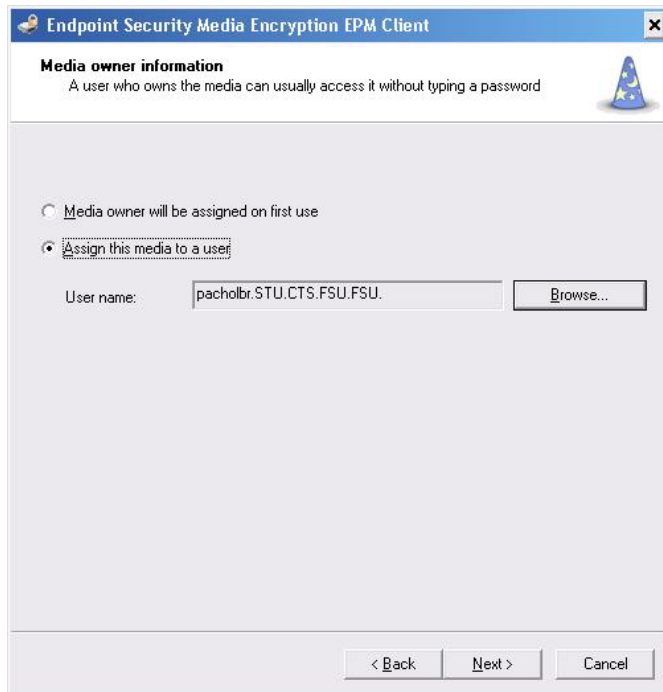
1. If you haven't already, log into Novell before plugging in your media device. This is **essential** to ensuring that your media device is encrypted under your own account.
2. When you plug in a media device, like a flash drive, you should see the message below pop up. Click **Next**.



3. If your media device has very sensitive data you can choose the secure format to perform multiple passes. Click **Next**.

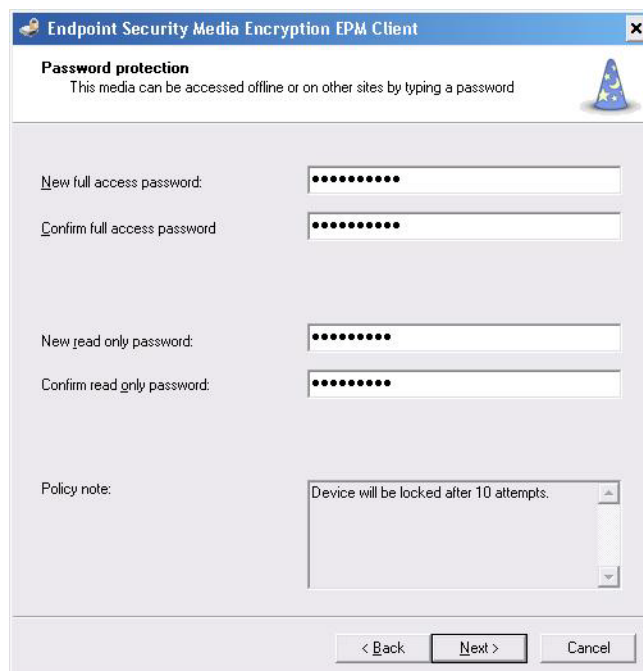


4. Click **Assign the media to a user**, and ensure that your user name appears



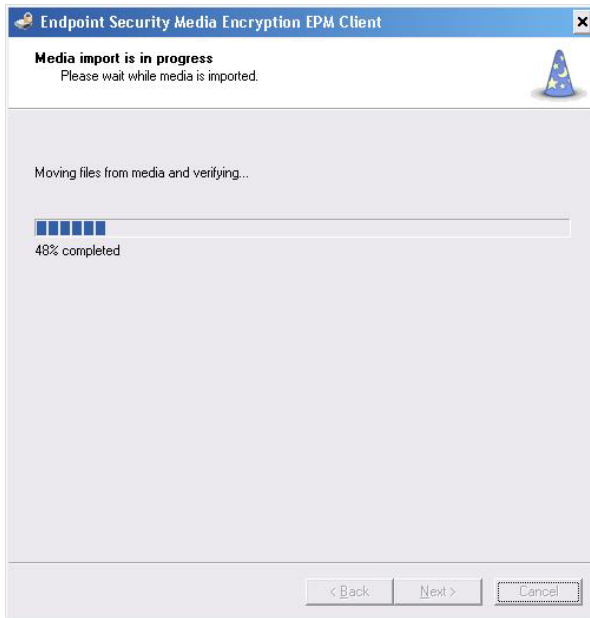
The screenshot shows a window titled "Endpoint Security Media Encryption EPM Client". The main heading is "Media owner information" with a sub-note: "A user who owns the media can usually access it without typing a password". There are two radio button options: "Media owner will be assigned on first use" (unselected) and "Assign this media to a user" (selected). Below the selected option is a text input field containing "pacholbr.STU.CTS.FSU.FSU." and a "Browse..." button. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

5. Next, you will be asked to create 2 passwords. The first password will grant full access and the second will only allow viewing, not changing, of the information on your device. Both passwords must be at least 8 characters long and contain at least one uppercase letter and one number. Click **Next**.

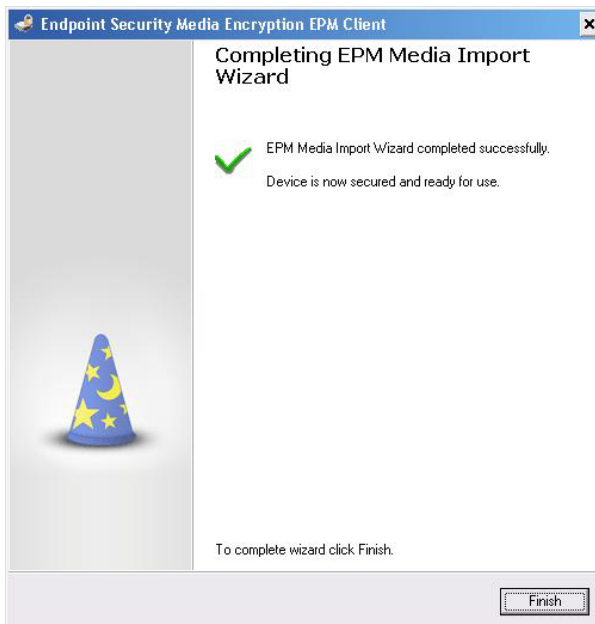


The screenshot shows a window titled "Endpoint Security Media Encryption EPM Client". The main heading is "Password protection" with a sub-note: "This media can be accessed offline or on other sites by typing a password". There are four password input fields, each with a confirmation field below it: "New full access password:", "Confirm full access password:", "New read only password:", and "Confirm read only password:". At the bottom left is a "Policy note:" label next to a text area containing "Device will be locked after 10 attempts.". At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

6. A progress bar will appear as the encryption proceeds.



7. Click **Finish** when the screen below appears.



If you have any questions please call the Technology Assistance Center at 231-591-4822.

How do I remove the encryption from my media device?

Plug the memory card into your laptop and copy its contents onto your desktop. When the device is empty click **Start**, then **My Computer**. Navigate to and right click the drive that corresponds to your device, and select **Format...** Click **Start**. Your media device is no longer encrypted, and you can copy its previous contents back onto it.

Am I able to plug an encrypted drive into a computer that does not have the MDE client installed on it?

Yes. Simply enter your MDE password after plugging your device in.

Am I able to plug a non-encrypted drive into a computer that does have the MDE client installed on it?

Yes, you will first be prompted to encrypt the drive. If you do so then you will gain full access to the drive. If you choose not to encrypt then you will still be able to access your drive but with read-only access. This means that you will be able to view and open documents but you will not be able to modify them or transfer new files onto the drive.

Am I able to reset my password on a MDE encrypted device?

Yes. See the FAQ above about resetting your password.

What is Read-only access?

Read-only access commonly refers to file permissions or the rights that you have to files or folders. When you have read-only access to a file you will be able to view the file, open the file, copy and paste the file to a different location, but not make changes to the file. Also, you cannot save files to a media device that has read-only access.

Is it possible to recover files that have been deleted from an encrypted drive?

No, once a file is deleted from an encrypted drive it is unrecoverable.

Why isn't my device reading its memory card?

If you have encrypted the memory card on your laptop, it will not be accessible by the device (camera, phone, camcorder etc.). You will have to plug the memory card back into your laptop and copy its contents onto your desktop. When the device is empty, click **Start**, then **My Computer**. Navigate to and right click the drive that corresponds to your device, and select **Format...** Click **Start**. Your media device is no longer encrypted, and you can copy its previous contents back onto it.

Can I plug my iPod into my encrypted computer?

You can read from an iPod and play music through iTunes. You will not be able to place music onto the device. You should choose not to encrypt this device.

Can I plug my BlackBerry into my encrypted computer?

You can place images, music, and documents onto the device's internal memory. If the BlackBerry has an SD memory card, the media encryption software will try to encrypt the card. You should choose not to encrypt this device.

Can I plug my SmartPhone into my encrypted computer?

You can place images, music, and documents onto the device. Check Point does not recognize an SD memory card inserted into the phone, so it does not try to encrypt the added storage.