EEFF – USB Administrative Recovery

ePO and Endpoint Encryption

Desktop Services

Introduction

McAfee Endpoint Encryption for Files and Folders (EEFF) provides the capability to encrypt removable media. The most common configuration is to create an encrypted container on the removable device and store all data in that encrypted container (rather than encrypting individual files); this is referred to as EERM. If a user were to forget their password for this encrypted container, they would need a way to unlock the device and reset their password. EEFF allows a few options for this (like using a backup password or using a certificate on smartcard), but the most common recovery method is to use a key that is stored on the user's computer. This way, all the user has to do is insert their USB stick into their computer that is running EEFF and click the recovery button. Since the recovery key is on that system, EEFF knows to use that key to unlock the device and let the end user update their password. This is a good way of approaching the problem because it allows the user to reset their password without having to make a helpdesk call. This recovery key can be a shared key (which would allow the user to perform the recovery operation from any managed system in your environment) or a personal key (which only allows the user to perform recovery from their own system). It is most common to use a personal key. The process for configuring EEFF to perform EERM encryption and use personal keys for recovery is documented here:
https://community.mcafee.com/community/business/data/epoenc/blog/2012/12/19/how- to-handle-removable-media-encryption-with-endpoint-encryption-for-files-and-fold ers-41

Administrator Recovery

While user personal keys provide an easy and secure way for end users to reset their own password, they pose a problem for administrators. If an administrator were to find one of these USB sticks laying on the ground, they would not have immediate access to it because they don't know the user's password and they don't have access to the user's personal key (since it is only distributed to the user). Of course the administrator could simply format the device and use it for another purpose, but if their was a business need to recover the data they would need to follow these steps to get access to the data.

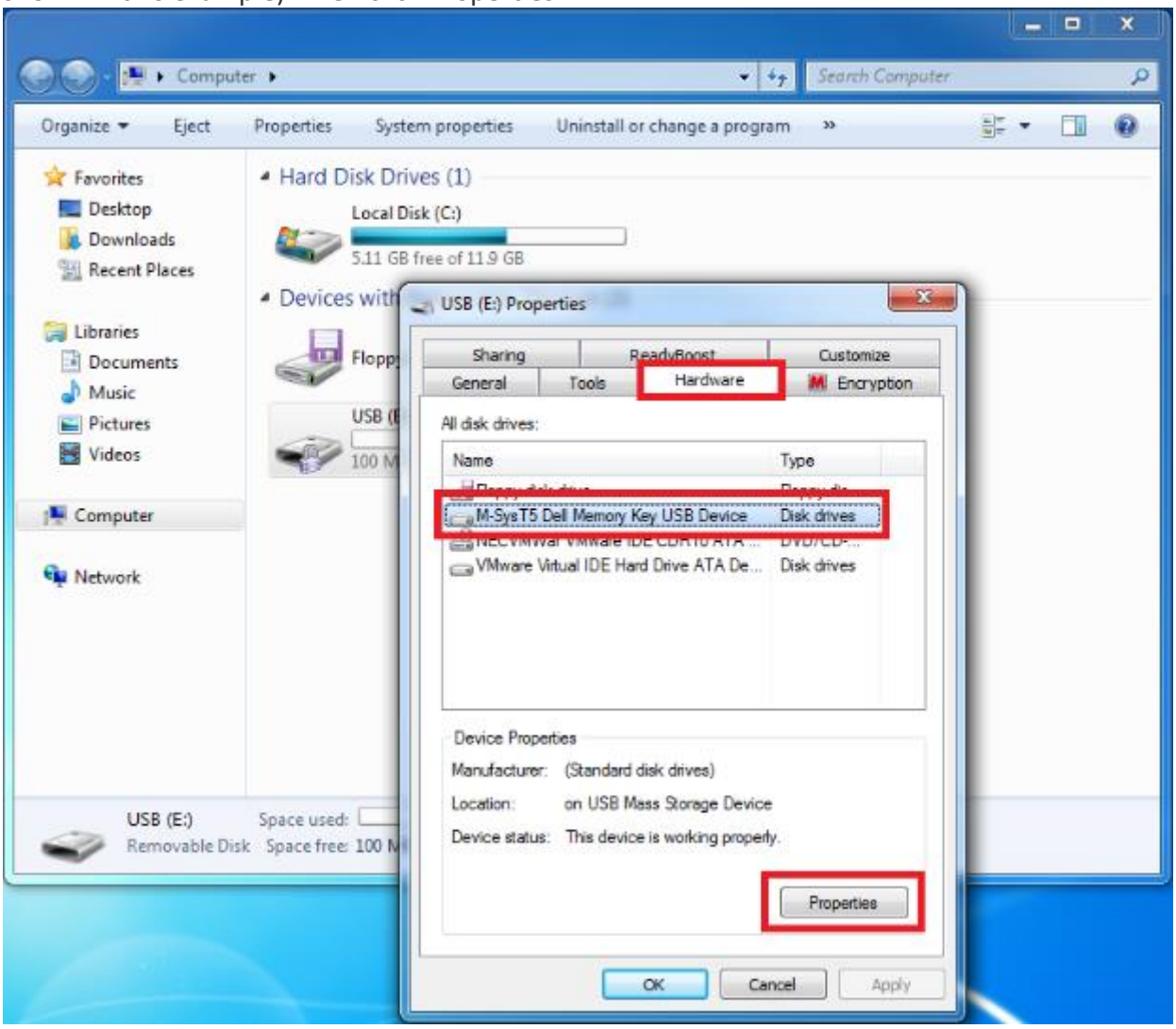
High Level Overview

- Determine the removable media device's serial number
- Make a query in ePO that identifies all events for that device; one event will show which user encrypted the device
- Locate the user personal key for that user and convert it to a regular key
- Grant the administrator access to that key
- Synchronize the administrator's system with ePO so that they key is delivered to the administrator's system
- Insert the device into the administrator's system and use the key to unlock the device

Note: This is only possible with EEFF 4.1 and later because EERM reporting only exists in those versions.

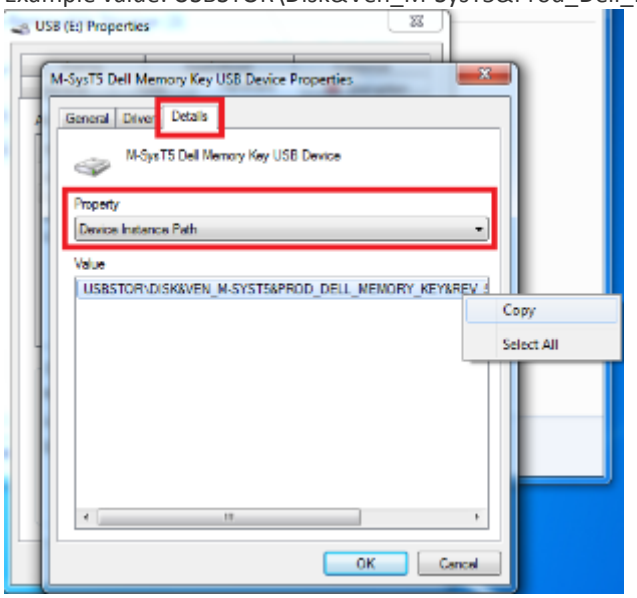
Step By Step Process

1. Insert removable media device into a Windows computer
2. Open Windows Explorer, locate the removable media device and right click on it. Then choose properties.
3. Select the Hardware tab. Select the removable media device (M-Sys T5 Dell Memory Key is shown in this example). Then click Properties.

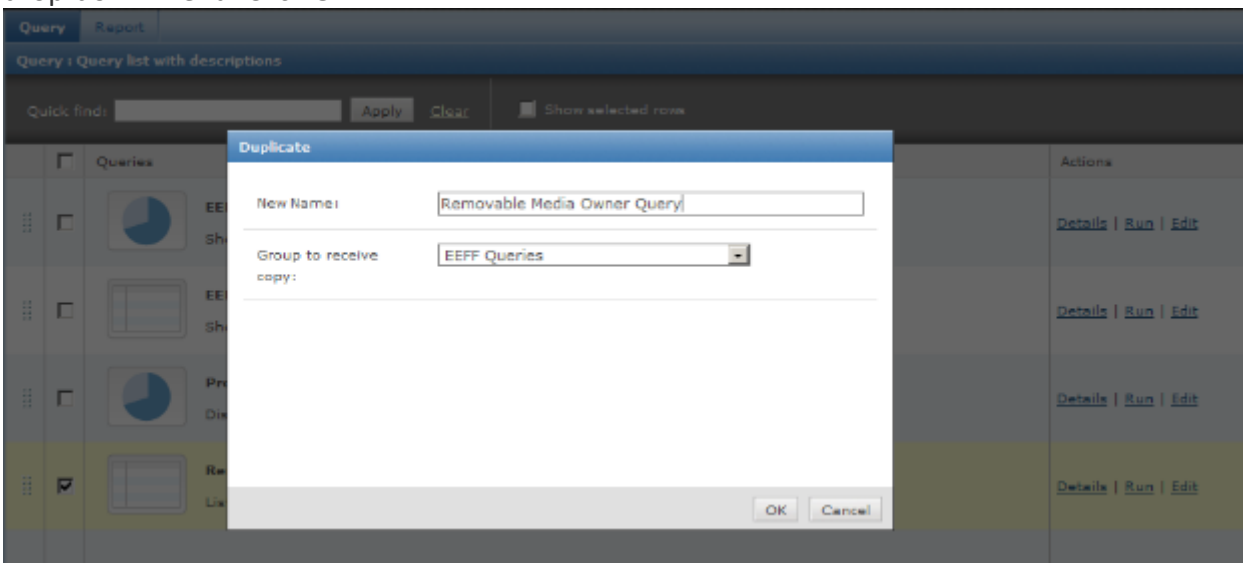


4. Select the Details tab. In the Property drop-down menu, choose "Device Instance Path." Right click on the Value and choose copy. We will need to paste this into ePO later, so keep it in the clipboard or paste into a Notepad file for temporary storage.

Example value: USBSTOR\Disk&Ven_M-SysT5&Prod_Dell_Memory_Key&Rev_5.00\07D16450B19148E7&0



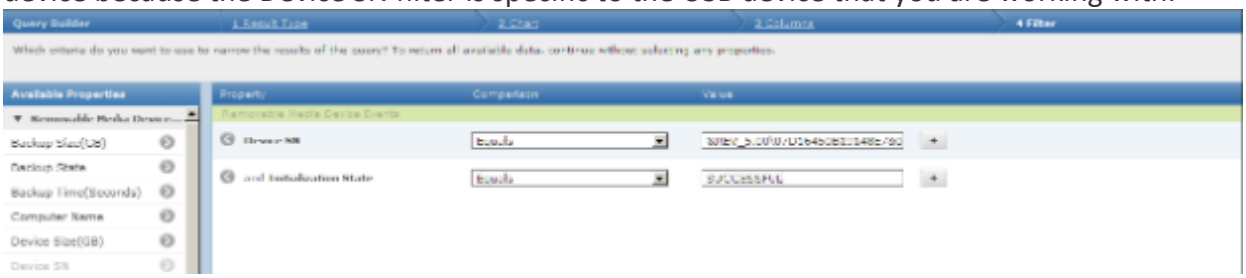
5. Log in to ePO
6. Go to Menu > Reporting > Queries & Reports
7. Expand the Shared Groups list and select EEFF Queries
8. Check the box next to the query titled Removable Media Device Events
9. Select Actions > Duplicate
10. Name the new query Removable Media Device Owner Query. Select EEFF Queries from the drop-down menu. Click OK.



11. Find your new query in the list and click Edit
12. You will arrive in step two of the query building process, labeled as "2 Chart." No changes are needed here, so click Next to proceed.
13. On step three of the query building process, our goal is to reduce the number of columns included. We only want to retain User Name, Device SN, Computer Name, Initialization State, Product Name, Protected, and Event Generated Time. Click Next to proceed.

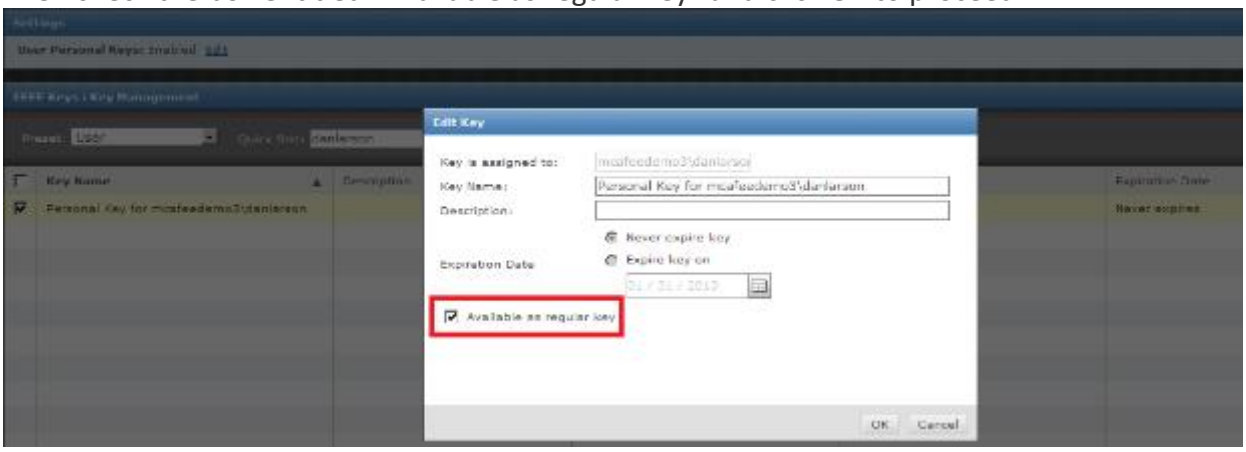
14. Step four of the query building process is where we will limit the query to only return events for the removable media device that we are interested in. This is done by filtering on two properties. First select Device SN. Set the drop-down menu to Equals. Then type the device serial number (also known as Device Instance Path) that was collected in step four (above). The next property to include in the filter is Initialization State. Set the drop-down menu to Equals and type SUCCESSFUL into the value field. Including this filter will limit the query's results to the event that includes the username of the person who encrypted the USB device. This is critical since the rest of the process is only possible if we identify this user's personal key. Click Save to save the query. Click Save again to finish the process and to return to the list of queries.

    Note: This query will need to be edited every time you want to unlock a new removable media device because the Device SN filter is specific to the USB device that you are working with.

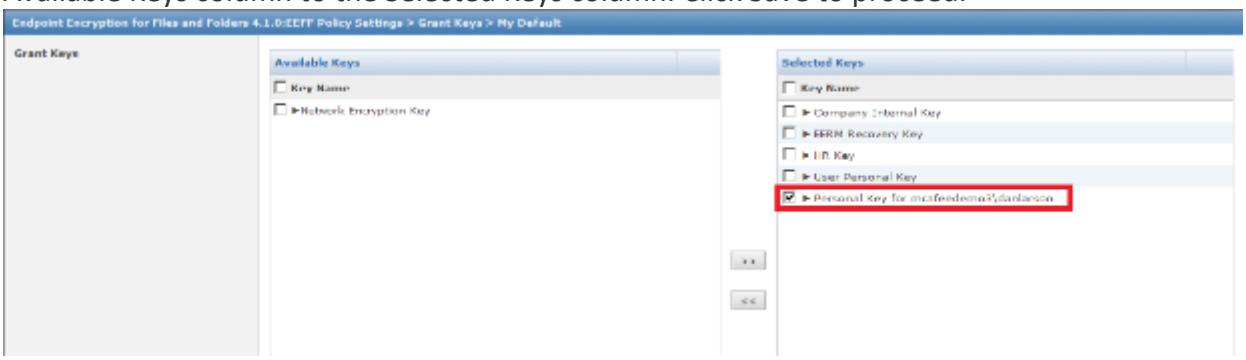


15. Find the query in the list and click Run
16. Validate the query results and make note of the User Name.
17. Go to Menu > Data Protection > EEFF Keys
18. From the Preset drop-down menu, select User. This will return a list of all User Personal Keys in the environment.
19. Enter the user name from your query into the Quick find field and then click Apply.
20. Check the box next to the key name
21. Click Actions > Edit Key

22. Then check the box entitled "Available as regular key" and click OK to proceed



23. Go to Menu > Policy > Policy Catalog
24. Select Endpoint Encryption for Files and Folders from the Product drop-down menu
25. Select Grant Keys (UBP) from the Category drop-down menu
26. Select the Grant Keys policy that is assigned to your administrator
27. Select the personal key that was changed to a regular key in step 22 (above). Move it from the Available Keys column to the Selected Keys column. Click Save to proceed.



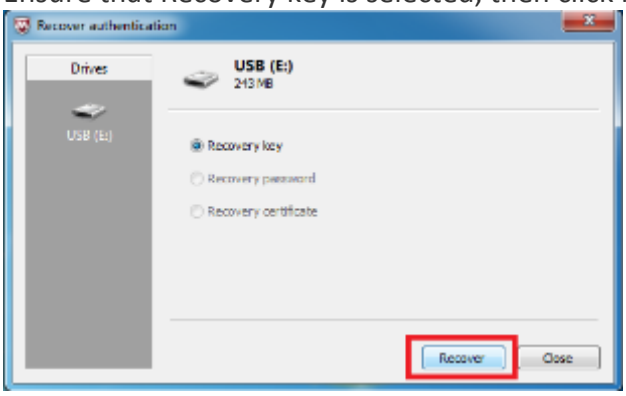
28. Synchronize the administrator's system with ePO. This will detect the updated policy and deliver the new key.
29. To validate that the key has been delivered, right-click on the McAfee Agent. Select Manage Features > Endpoint Encryption for Files and Folders. Then expand the Available keys menu. The key will be identified as a Personal Key and it will contain the original user's domain and username.

    Note: This process will only work on systems where the original user (danlarson in this example) has never logged in.

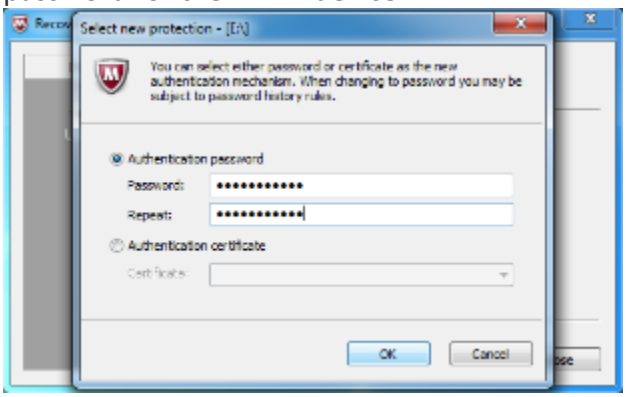
30. Insert the EERM Encrypted removable media device

31. On the EERM login screen, choose Recover ...

32. Ensure that Recovery key is selected, then click Recover



33. The EEFF client will now automatically use the converted user personal key to unlock the device. Once the device is unlocked, the administrator will be prompted to create a new password for the EERM device.



34. If the new password is valid, the administrator will receive confirmation

35. The device is now unlocked and its data is accessible to the administrator. You can access the data by simply browsing to the device in Windows Explorer.

Source: https://community.mcafee.com/community/business/data/epoenc/blog/2013/01/31/how-to-recover-data-on-usb-sticks-encrypted-with-eerm