McAfee Edge Admin Guide

ePO and Endpoint Encryption

Desktop Services

Introduction

What is McAfee Endpoint Encryption

McAfee Endpoint Encryption provides superior encryption across a variety of endpoints such as desktops and laptops. The Endpoint Encryption solution uses strong access control with Pre-Boot Authentication (PBA) and a NIST approved algorithm to encrypt data on endpoints. Encryption and decryption are completely transparent to the end user and performed without hindering system performance. Administrators can easily implement and enforce security policies that control how sensitive data is encrypted. These policies allow the administrators to monitor real-time events and generate reports to demonstrate compliance with internal and regulatory requirements. Endpoint Encryption has the advantage over other competitive encryption products, because it engages encryption prior to loading of the Windows or Mac operating system, while data is at rest.

What is the ePO Server

The McAfee ePO (e-Policy Orchestrator) server is an endpoint management server. The McAfee ePO server manages Endpoints which have had the McAfee Agent installed on them. ePO is used to monitor endpoints, deploy encryption policy and deploy encryption extensions. In order to deploy and enable McAfee Endpoint Encryption you will need to access the ePO server through the link below.

Accessing the ePO Server

Edge Administrators will need to perform a number of tasks through the McAfee ePO server to manage the encryption state of Endpoints in their area. To login to the McAfee ePO server follow the steps below…

McAfee ePO server address:

https://137.82.116.22:8443

Login Credentials:

Username: **ead\CWLAdminID**
Password: **Your CWLAdminID password**

If you are an edge admin and your supported area utilizes the McAfee Endpoint encryption product you should already be setup to login to the ePO server. If you cannot login to the server please open a ticket @ http://it.ubc.ca/sos and access will be provided.

Firewall Exceptions:

You need to prepare your systems to allow ePO to connect and configure your computers and to allow traffic to return through any institutional border firewall or port blocking that you may have in place.

Ports Used:

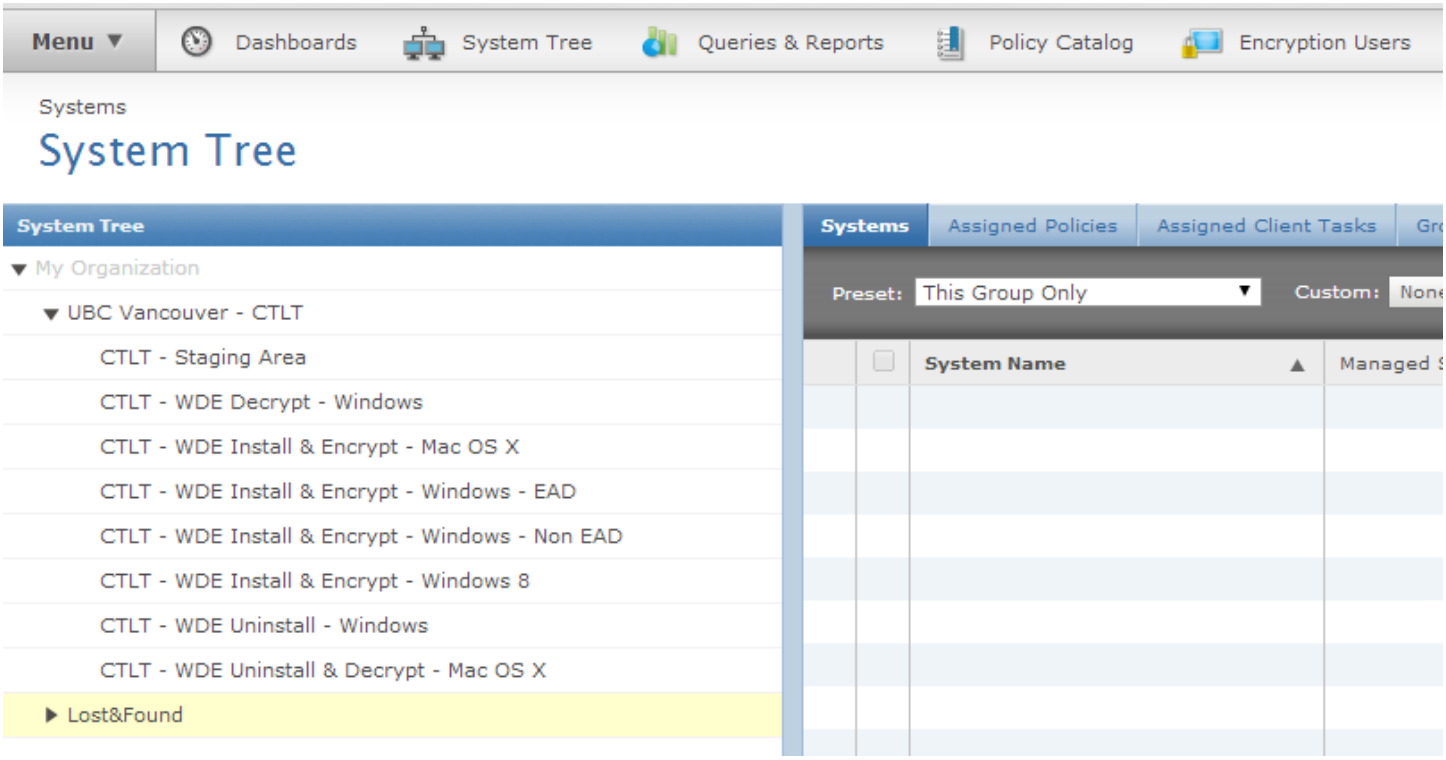
Agent to server communication is via port 443 by default, so typically should not be impeded. For Admin access you will need to be able to access the following URL: https://encrypt.it.ubc.ca:8443

Service Ports table:

Service	Port	TCP/UDP
Bi-directional Agent to Server communication.	80	TCP
Bi-directional Agent to Server secure communication	443	TCP
Agent Wake-up communication port opened by agents to receive agent wake-up requests from the ePO server.	8081	TCP
Inbound Agent broadcast communication	8082	UDP
Console-to-application server communication port. Inbound connection to the ePO server from ePO Console.	8443	TCP
Bi-directional Client to server authenticated communication	8444	TCP
Security threats communication port	8801	TCP

Groupings within ePO

McAfee utilizes groups within ePO to manage policy assignment for managed endpoints. Permission sets are create to assign Edge Admins access to manage only their own supported groups. This allows Edge admins to manage policy assignment, policy creation, endpoint monitoring, group creation for their group and gives the feel that they are working off their own server. Other edge admins will not have access outside of their supported group this helps to ensure that your endpoints are as secure as possible and information on the endpoints cannot be viewed by any other Edge Admins. Below is an example of how your ePO groupings will be configured when you first log into the server…



All Endpoints which have the McAfee agent installed will initially show up in the Staging Area folder in the left pane. Machines are sorted using by the group that you have selected during the creation of the McAfee SmartInstaller.

For machines which do not fall within sorting criteria the Lost & Found folder is where these machines will appear. The Lost & Found group is open to all edge admins and as such we ask that you monitor this folder to be sure that you do not have any stray machines within it. Once a machine appears in the lost and found it will need to be moved into the Staging Area group.

Note: Installing the McAfee agent does not mean that encryption is enabled. McAfee pushes all encryption extensions to endpoints once they have been moved into one of the defined groups.

ePO Defined Groups

Each sub-group is setup with predefined groupings. Each grouping is configured with Assigned Policies and Assigned Client Tasks. When an Endpoint is moved from the Staging Area group to one of the predefined groups the Policies and tasks for each group is pulled from the server to the client.

ePO Assigned Policies and Assigned Client Tasks

Assigned Policies

Assigned Policies are setup on each group within ePO and these are what sets requirements for encryption such as Product settings, User Based Policies, Removable Media Settings and McAfee Agent Settings. All of these settings and policies are what defines how the McAfee Endpoint Encryption Product Functions.

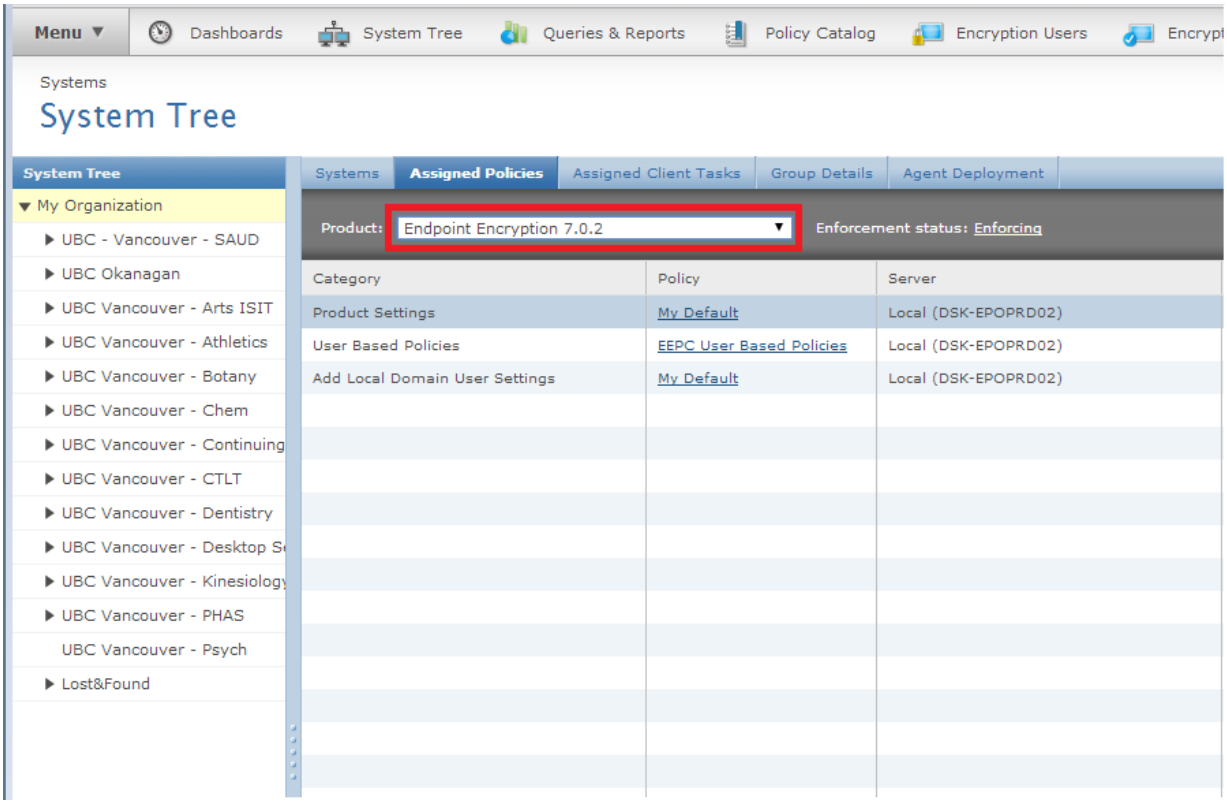
Assigned Client Tasks

Client tasks are assigned to each subgroup and this section is what handles Client install, encryption agent install as well as deploying hotfixes and updates to client Endpoints. These items are predefined and cannot be modified by edge admins.

Managing computer policies:

1. Log on to the ePO console.
2. Click **System Tree**.
3. Under **System Tree**, select the group that the computer to be managed resides in.
4. Click the **Assigned Policies** tab and select the product to be managed for the selected computer(s) from the drop-down.

   NOTE: Each product has its own set of policies. These policies can be found by clicking the Product drop down menu at the top of the page.



5. Under the **Actions** column, click **Edit Assignment** to create a product-specific custom policy for the selected group.
6. To the right of **Inherit from**, select **Break inheritance and assign the policy and settings below** to configure custom policy settings.

7. To the right of **Assigned policy**, select **one** of the following:
    - **Existing policy from the drop-down:**
        1. Click **Edit Policy**
        2. Make the desired changes and click **Save**.
    - **New Policy**:
        1. Click **New Policy**.
        2. Specify a name to create a new custom policy setting and click **OK**.
        3. Make the desire changes and click **Save**.

8. To the right of **Lock policy inheritance**, select the desired option to either allow or prevent policy inheritance from being broken below the currently selected level.
9. Click **Save**.

Managing computer Tasks:

1. Log on to the ePO console.
2. Click **System Tree**.
3. Under **System Tree**, select the group that the computer to be managed resides in.
4. Click the **Client Tasks** tab and select **one** of the following:

    - **Manage Existing Task:**

        1. Under the **Actions** column, click **Edit Settings** for the desired task.
        2. Configure the setting changes under the **Description**, **Configuration**, **Schedule** and **Summary** tabs.
        3. Click **Save**.

    - **New Task:**

        1. Click **Actions**, **New Task**.
        2. Specify a name for the task.
        3. To the left of **Type**, select the type of task to run for the selected computer(s).
        4. Click **Next**.
        5. Under the **Configuration** tab, select the desired options and click **Next**.
        6. Under the **Schedule** tab, select the desired scheduling options and click **Next**.
        7. Under the **Summary** tab, review the settings.
        8. Click **Save**.

Managing User Access Assignment

Automatic Assignment – EAD Joined Windows Endpoints

Manually assigning individual users for each system in your environment would be a time consuming undertaking. EEPC automates this process with a new feature called Add Local Domain Users in the system settings policy. If enabled, the agent will enumerate the currently logged in Windows user and all the cached profiles on the endpoint. This data will then be sent to ePO and ePO will automatically provision those users to that system. This is the best way to provision end users to systems and should be done in almost all cases. Some special systems, like loaner laptops or classroom PCs, will require a different user provisioning strategy.

Note: For all EAD joined Windows 7 Endpoints the Automatic Assignment Policy is preconfigured so no technical interaction is required. For clients who are not joined to EAD the Individual Assignment process will be required.

Individual Assignment – Add a single user to an Endpoint

1. Log into ePO
2. Go to **Menu** | **Data Protection** | **Encryption Users**
3. Select the Endpoint you wish to assign a user to
4. On the bottom of the page click **Actions** | **Endpoint Encryption** | **Add Users**
5. Click on the icon to the right of the **Users** field and search for the CWL ID of or the name of the user you would like to grant login access to the Endpoint.
    a. **Note: Be sure to adjust the search options to search both Container and Children.**
6. Click OK when done.

Assigning a Role/Permission Group Login Access

As a support technician you may find it necessary to add your Admin-Tech group to have login access to all Endpoints within your supported group. You may also have some Endpoints within your group which are accessed by all users such as loaner laptops or meeting room computers. See below for steps on how to add a Group of users to a single endpoint or a group of endpoints…

Add a Group of users to access all computers within an ePO group. (Technician Access)

1. Log into the ePO server
2. Go to **Menu** | **Data Protection** | **Encryption Users**
3. Select your group in the left hand column, I.e. **UBC Vancouver – Your Group**
4. In the right hand column click on the **Group Users** tab
5. Use the Actions button at the bottom and go to **Endpoint Encryption** | **Add Users**

6. Click on the icon to the right of the groups field and search for the role/permissions group which you would like to have access to the Endpoints.
    - Note: due to the large number of groups some areas have it is easier to search the domain tree on the left hand side of the screen. Find your group and select it from the pane on the right and click ok.
    - If your group has nested groups inside it be sure to click the checkbox for recursive rights.
7. Click **OK** when done.

Add a Group of users to access a single computer. (Loaner computer)

1. Log into ePO
2. Go to **Menu** | **Data Protection** | **Encryption Users**
3. Select the Endpoint you wish to assign a group of users to
4. On the bottom of the page click **Actions** | **Endpoint Encryption** | **Add Users**
5. Click on the icon to the right of the **Groups** field and search for the group of users you would like to have login access to the Endpoint.
    - Note: due to the large number of groups some areas have it is easier to search the domain tree on the left hand side of the screen. Find your group and select it from the pane on the right and click ok.
    - If your group has nested groups inside it be sure to click the checkbox for recursive rights.
6. Click OK when done.

To confirm that the user has been added to the Endpoint for access or to check who has access click **Menu** | **Data Protection** | **Encryption Users**, select the system you wish to check and using the Actions button at the bottom of the page select **Endpoint Encryption** | **View Users**.

USB Recovery Process

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 there was a business need to recover the data they would need to follow these steps to get access to the data.

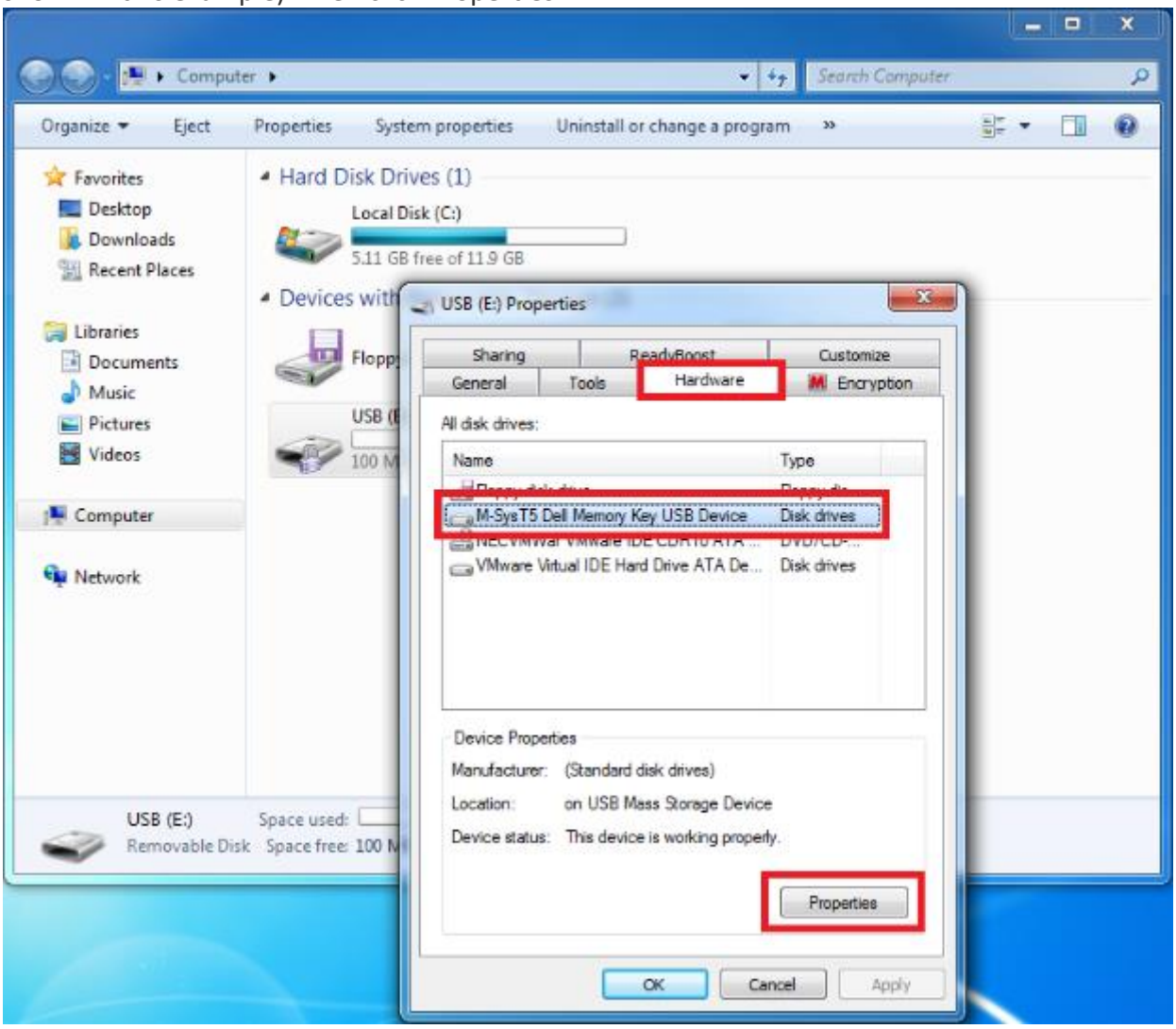
High Level Overview

- 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.

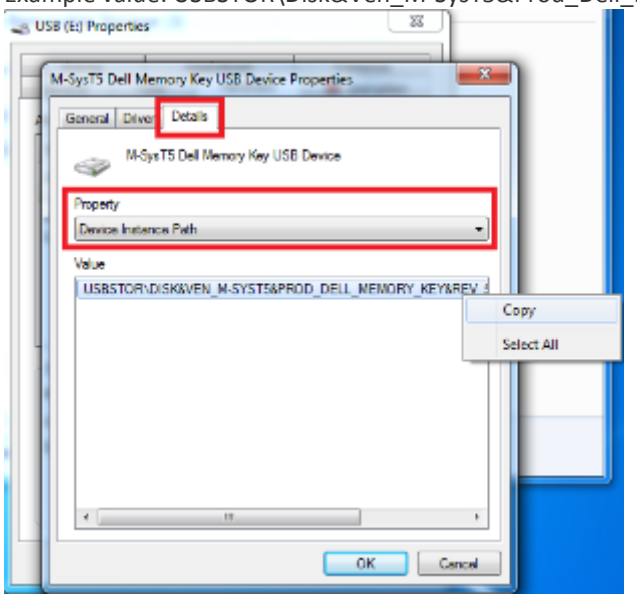
Step By Step Process

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.

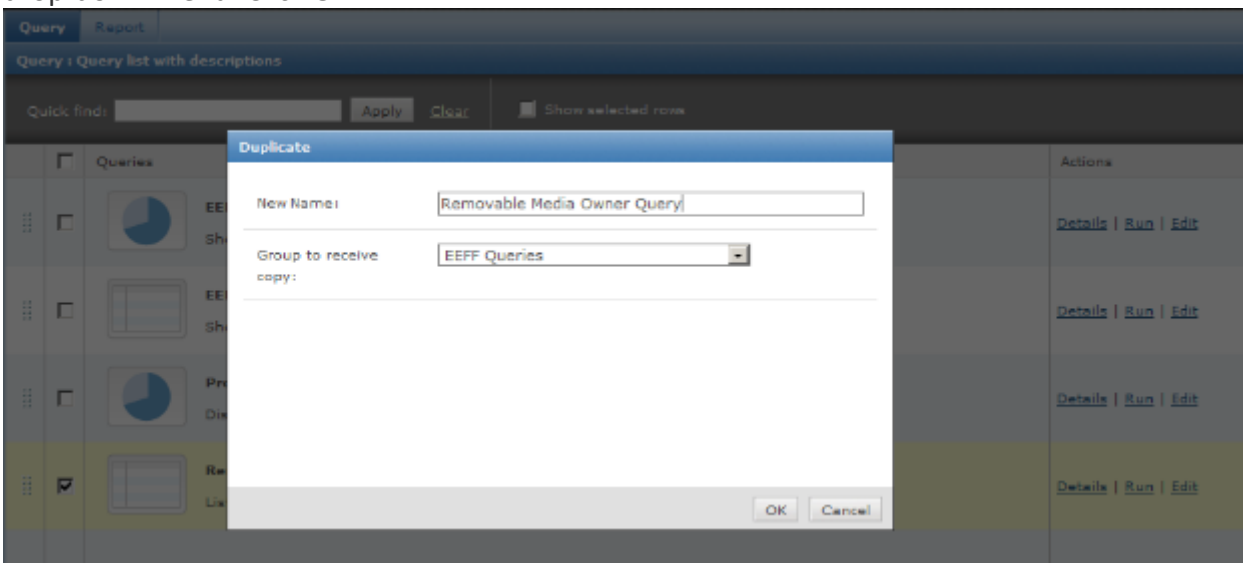


4. Select the Details tab. In the Property drop-down menu, choose "Device Instance Path." Right click on the Value and choose copy. We will need to paste this into ePO later, so keep it in the clipboard or paste into a Notepad file for temporary storage.

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



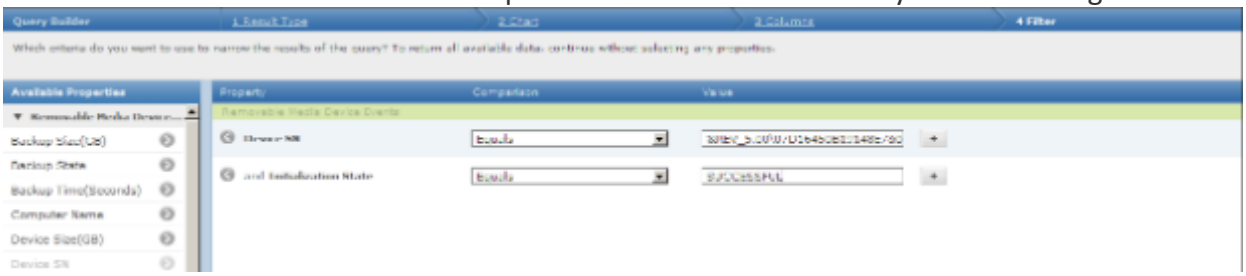
5. Log in to ePO
6. Go to Menu > Reporting > Queries & Reports
7. Expand the Shared Groups list and select EEFF Queries
8. Check the box next to the query titled Removable Media Device Events
9. Select Actions > Duplicate
10. Name the new query Removable Media Device Owner Query. Select EEFF Queries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

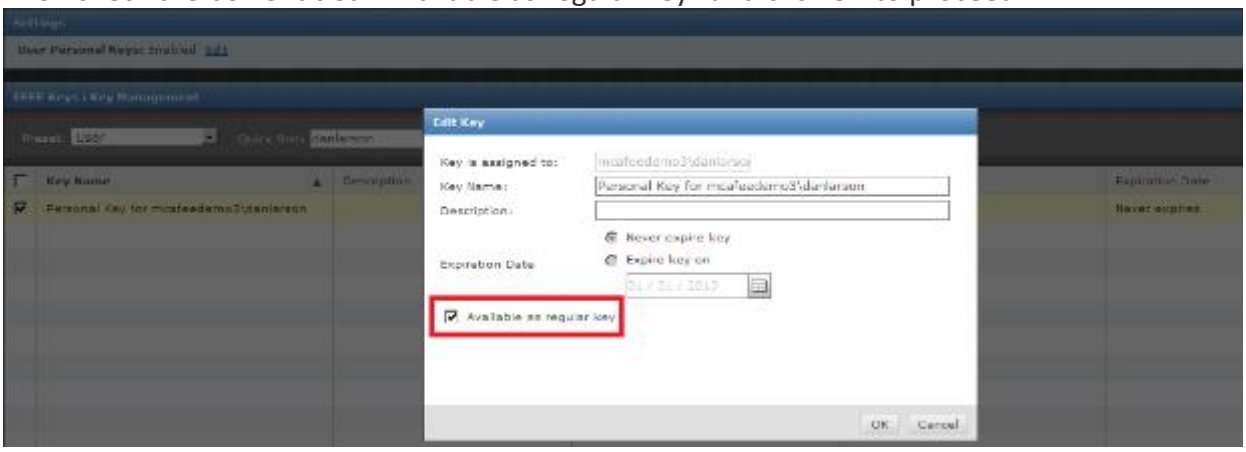
14. Step four of the query building process is where we will limit the query to only return events for the removable media device that we are interested in. This is done by filtering on two properties. First select Device SN. Set the drop-down menu to Equals. Then type the device serial number (also 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.

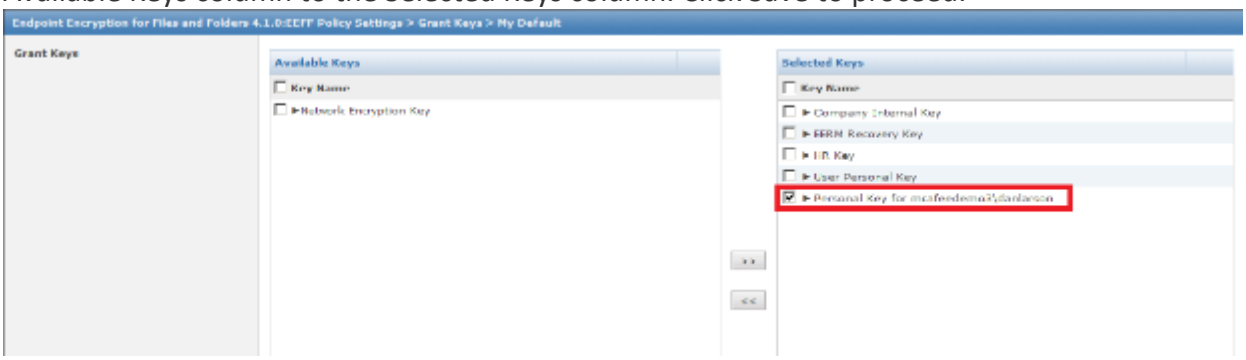


15. Find the query in the list and click Run
16. Validate the query results and make note of the User Name.
17. Go to Menu > Data Protection > EEFF Keys
18. From the Preset drop-down menu, select User. This will return a list of all User Personal Keys in the environment.
19. Enter the user name from 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.



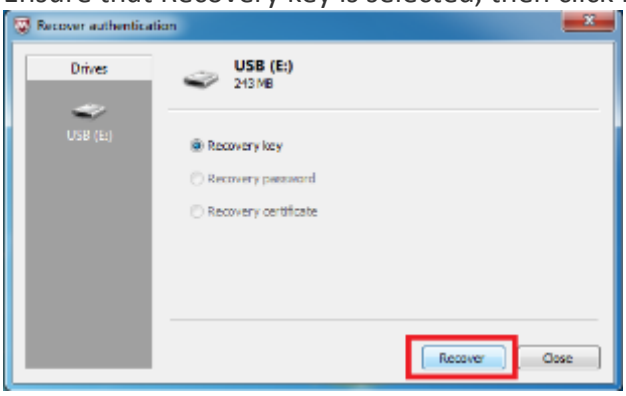
28. Synchronize the administrator's system with ePO. This will detect the updated policy and deliver the new key.
29. To validate that the key has been delivered, right-click on the McAfee Agent. Select Manage Features > Endpoint Encryption for Files and Folders. Then expand the Available keys menu. 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.

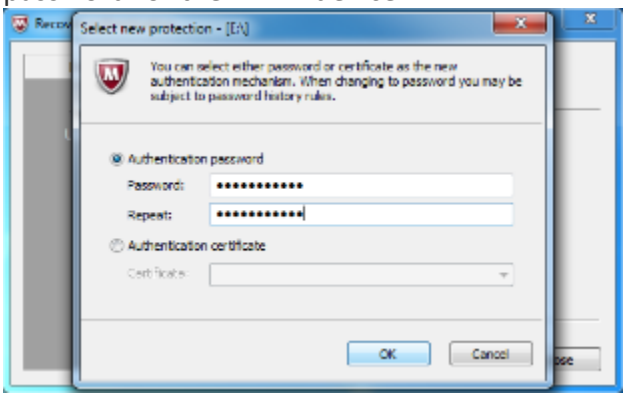
30. Insert the EERM Encrypted removable media device

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.



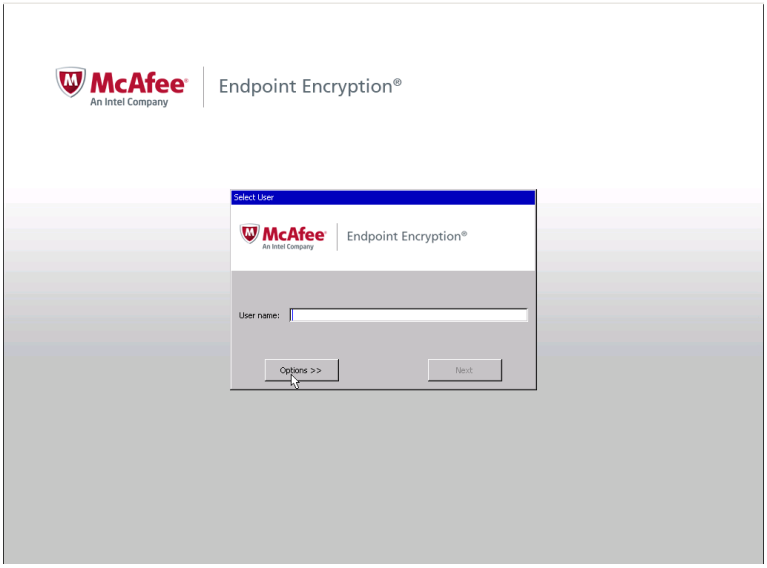
34. If the new password is valid, the administrator will receive confirmation

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

Machine and User Recovery

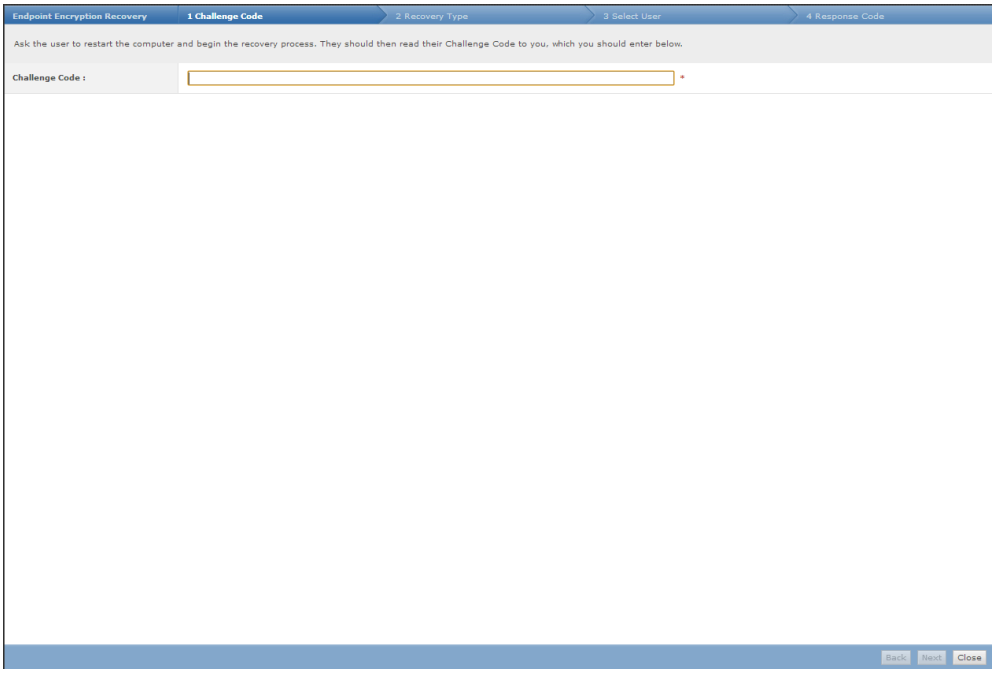
1. Instruct the client to boot the machine to the McAfee Login screen and click **Options**.



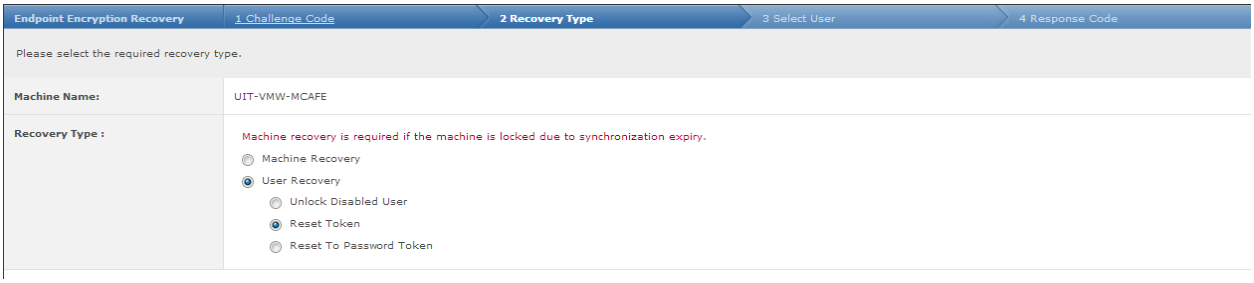
2. Instruct the client to select the **Administrative Recovery** Radio Button and click **OK**.

3. Once the client clicks the **OK** button they will be shown the client code for this session. Have the client read this code aloud. To read phonetically read the lines from Left to Right and Top to Bottom in order.

4. Enter the client code into the challenge code line as the client reads it out. Once entered click **Next**.

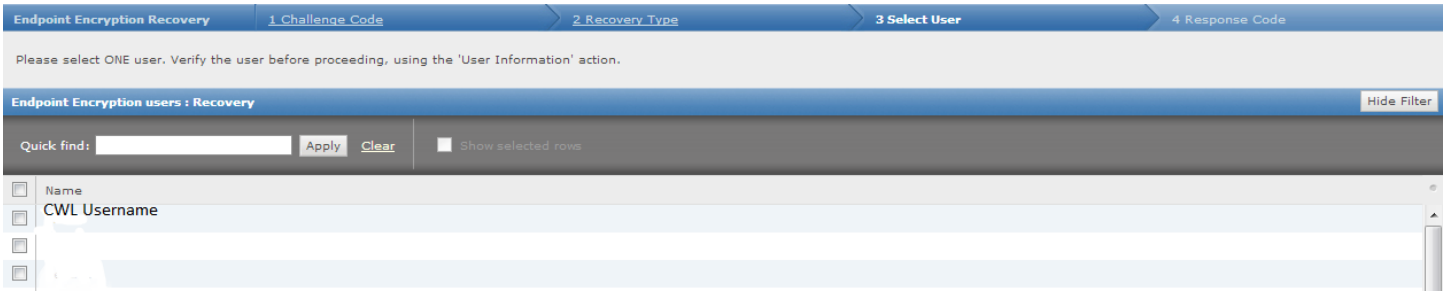


5. Select **User Recovery** | **Reset** Token then click Next.

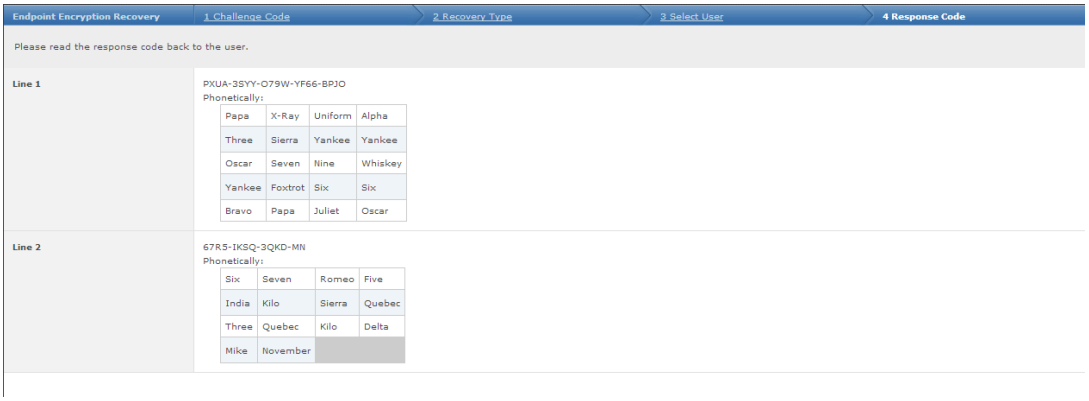


Note: Because we do not lock machine accounts the **Machine Recovery** option will not be used. The only time that machine recovery would be used is in the event of an Authorized user account not being present on the machine.

6. On the next screen confirm the username with the client. Once the client is able to provide you with the Username from the list and you can confirm their identity click the Checkbox beside the Username and click **Next**.



7. Read the Response code back to the client. Have the client enter the Code from line 1 into the provided boxes on their machine then click **Next**. Have the client enter the Code from line 2 into the provided boxes then click **Finish**.



8. Once the client has entered these codes and clicks finish they will immediately be prompted to create a new password. If there is an error have the client go back and re-enter the codes.
9. Confirm the client has created a new password then click Close in the lower right hand corner of the screen.