

The Circulation of Tenure Dossiers

2a. Encrypted USB Key

Our office, in consultation with IT Services, is recommending the use of a specific encrypted USB key for sharing the tenure dossier with Tenure Committee members. This specified USB key will ensure privacy and security of the confidential tenure materials. There should be one USB key per Tenure Committee member, per candidate. Consider developing a labelling system on the USB keys to track which committee member has which key.

Background

The Ironkey is a high-security memory key. Content on the drive is always encrypted. A password is always required to access files on the drive. If the incorrect password to the key is entered 10 times consecutively, the drive self-destructs. The device meets the US government's FIPS-140 standard for data protection.

The Ironkey works like any other memory key except that it ALWAYS requires a password to access the files stored inside. The Ironkey may be set to lock automatically if dormant for a defined time to reduce potential document exposure if a device is left unattended.

Purchasing an Ironkey

The Ironkey storage drive will be available for purchase at the U of T Bookstores. To purchase these keys, contact Penny De Geer and reference the catalogue numbers below to receive a quote:

Penny De Geer
Technology Buyer & Departmental Software Licensing
pdegeer@uoftbookstore.com
416.640.5816

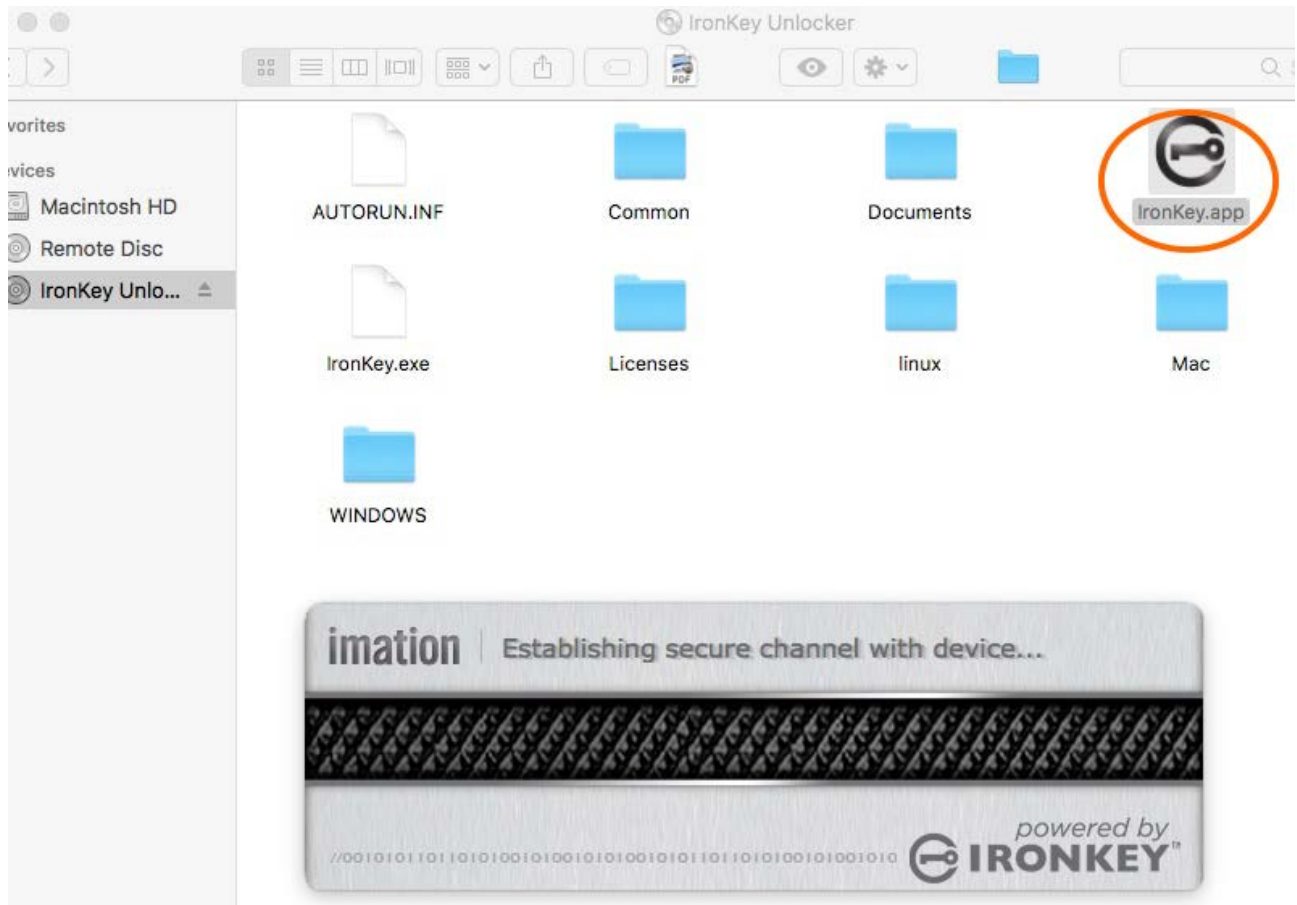
4GB IronKey catalogue number: IKD 300-4-GB

8GB IronKey catalogue number: IKD 300-8-GB

When choosing the size of the USB key, be mindful of the amount of materials that will be collected, and what size these files may be; e.g., if there will be any large visuals that will substantially add to the total file size.

Using an Ironkey

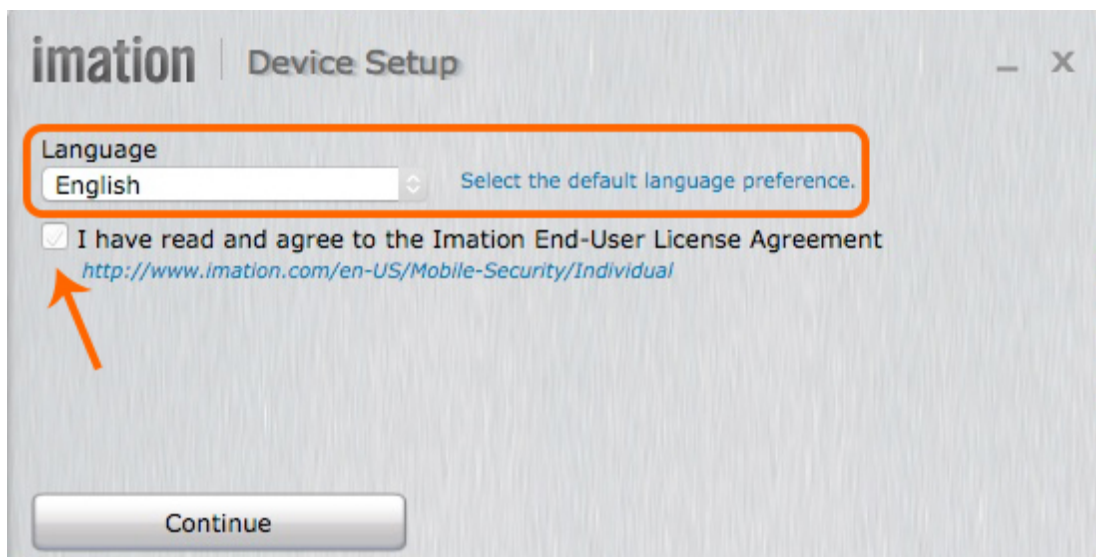
1. The Ironkey is initialized by the client by launching the Ironkey App when a new key is inserted into their computer's USB port. Upon launch of the Ironkey App, the device establishes a secure channel between it and the host computer and commences the setup process.



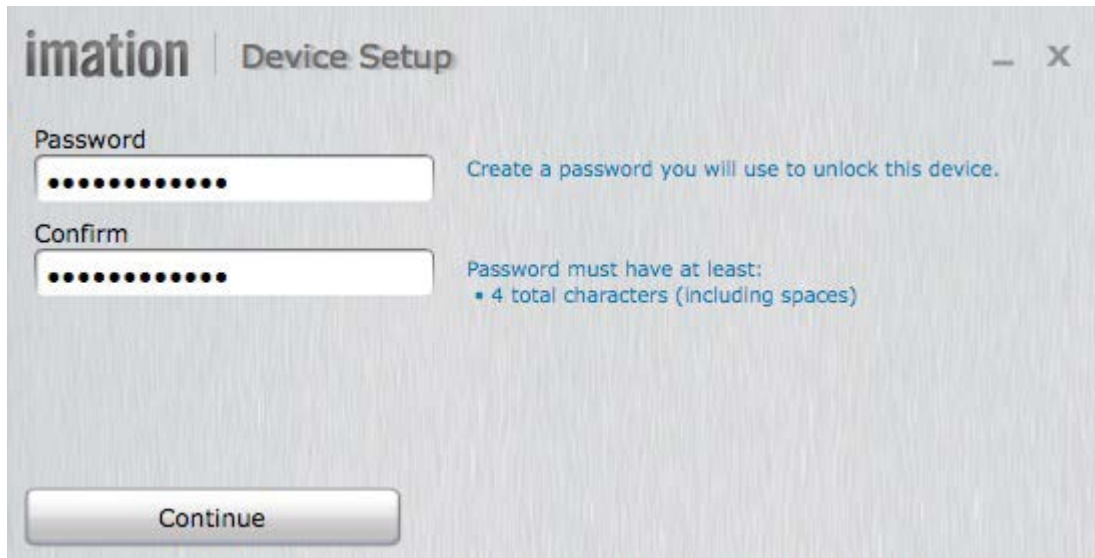
The device may be set up to work on Mac OSX, multiple versions of Windows, and Linux.

2. When the secure channel is established, the next screen in the setup process opens automatically.

On this screen, default language is selected from a drop-down list, and a check box appears for confirming the reading of the End-User License Agreement.



After clicking “Continue,” the device password is entered by the owner.



3. When the password is entered and validated, clicking “Continue” takes the owner to the data/device protection screen.

4. On this screen, options for device/data protection are selected:

- For the ***If I forget my password...*** box, selecting ***Reset the device instead of self-destructing*** causes the device to permanently delete the data following 10 consecutive incorrect password attempts, but preserves the Ironkey for future use.

- Not selecting ***If I forget my password...*** means that after 10 consecutive incorrect password attempts, the Ironkey encryption key will self-destruct and the device will become inoperable. **There is no way to recover the data or the key itself.**

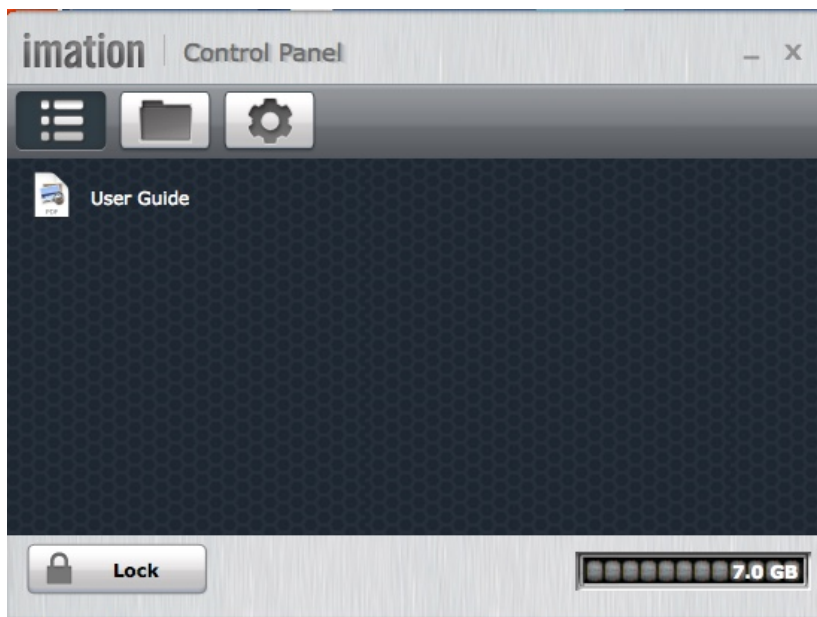
After “Continue” is pressed, the device configures itself.






5. Once the formatting is completed, the device is securely configured and ready for use.



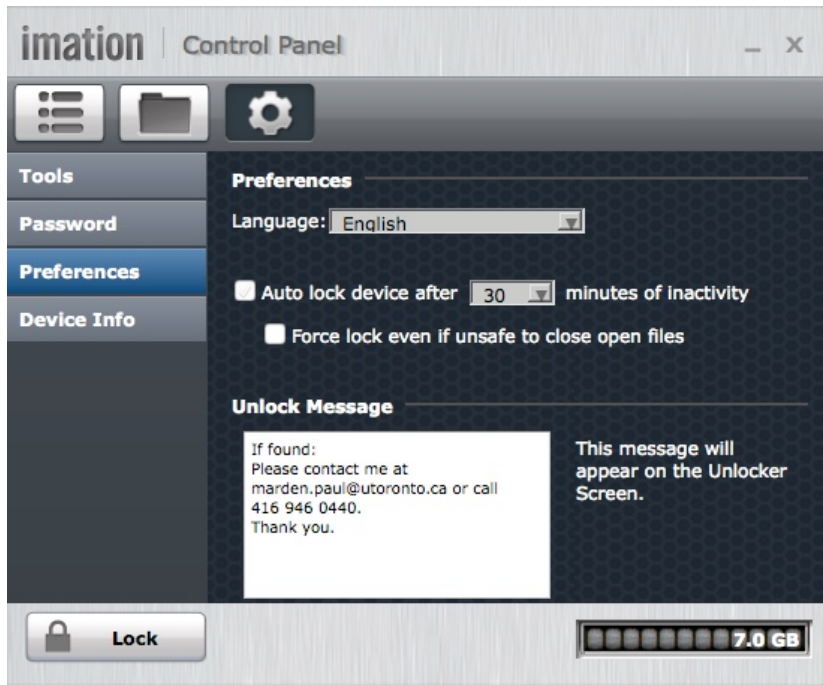
6. The Control Panel screenshot below is the main screen for accessing the device.



There are three icons at the top left:

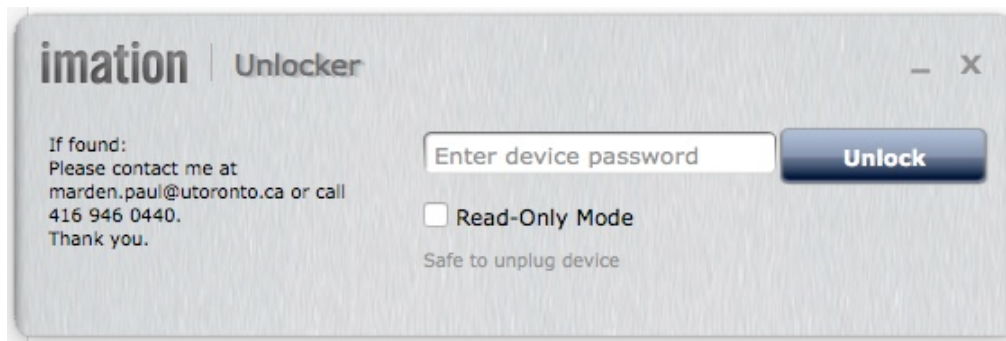
-  - The list icon represents the Ironkey's folder containing the owner's manual.
-  - The folder icon represents the main file folder in which the Ironkey stores files and subfolders.
-  - The gear icon represents the Settings option where changes may be made to the Ironkey password or self-destruct alternatives, as well as the "who to contact if my lost Ironkey is found by someone" and inserted into a USB port.

7. The lock icon closes and secures the Ironkey. The scale in the bottom right of the screen shows how much memory space is available on the key.



The device is now configured for future use.

8. Inserting the Ironkey into a USB port brings up the login screen below.



- Enter the password and click “Unlock.”
- Note the **If Found** text on the left.
- The Read-Only Mode checkbox is used when logging into an unfamiliar computer. This prevents any malware to be loaded onto the key until the machine’s integrity is checked, for example, by running a virus scan.

9. When the key is opened, the window shows files secured in the Ironkey. Files may be “dragged and dropped” into a folder or saved to the Ironkey directly.

Tenure Dossier Structure

It is recommended to upload materials as PDFs only to the USB key.

The file structure should be easily navigable for the Tenure Committee members; therefore, two methods are recommended:

- One large PDF with bookmarked sections; or
- Separate folders for each section which contain the relevant individual PDFs.

PDF With Bookmarks

A large PDF file can be created with all the required materials in the one file. Within the PDF, each section should be individually bookmarked. When choosing your bookmark structure, keep in mind the standard sections outlined in the [tenure dossier](#) segment of the AAPM that will be needed later when the tenure dossier is sent to the Provost's Office for review. Within each bookmarked section, it will be at your discretion how to organize the materials; for e.g., further sub-level bookmarks.

Folders Within the USB Key

Each key can be organized into relevant, easily navigable folders. When structuring the folders, keep in mind the standard sections outlined in the [tenure dossier](#) segment of the AAPM that will be needed later when the file is sent to the Provost's Office for review.

Once the Review is Complete

When the work of the Tenure Committee is complete, please be sure to collect the USB keys from each Tenure Committee member. Once the tenure review process is complete, delete the materials on each key, being careful to retain a full copy of the dossier for your records.

The USB keys can be kept for future use for other tenure dossiers.

Questions

If you have any questions on this method of circulating tenure dossiers, please contact the VPFAL Office at vp.fal@utoronto.ca.