

IRONKEY™ D300M SECURE USB 3.0 FLASH DRIVE

User Guide



ABOUT THIS USER GUIDE

This user guide covers the FIPS-Validated IronKey D300M and is based on the factory image with no implemented customizations. The examples used in this user guide are based on the IronKey™ EMS Default Policies.

System Requirements*

PC Platform

- Pentium III Processor or equivalent (or faster)
- 15MB free disk space
- Available USB 2.0 / 3.0 port
- Two consecutive drive letters after the last physical drive. See 'Drive Letter Conflict' on page 15.

PC Operating System Support

- Windows® 10
- Windows® 8, 8.1 (No RT)
- Windows® 7 SP1
- Windows® Vista SP2

Mac Platform

- 15MB free disk space
- USB 2.0 / 3.0

Operating System Support

- Mac OS X 10.9.x - 10.12.x

***NOTE: The IronKey D300M is a forced managed Secure USB Drive, IronKey™ EMS is required for managing these devices and is sold separately.**

Recommendations

To ensure there is ample power provided to the D300M device, insert it directly into a USB port on your notebook or desktop, as seen in **Figure 1.1**. Avoid connecting the D300M to any peripheral device(s) that may feature a USB port, such as a keyboard or USB-powered hub, as seen in **Figure 1.2**.



Figure 1.1 – Recommended Usage

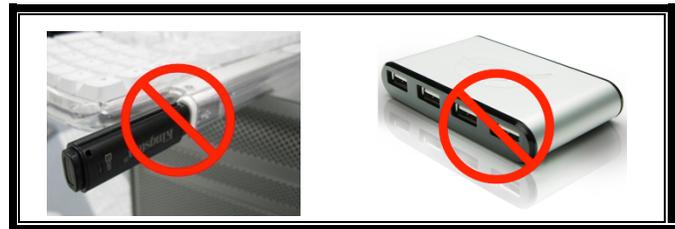


Figure 1.2 – Not Recommended

SETTING UP THE DEVICE (WINDOWS OS's)

1. Insert the D300M into an available USB port on your notebook or desktop and wait for Windows to detect it.
 - Windows users will receive a device driver notification as seen in **Figure 2.1**.

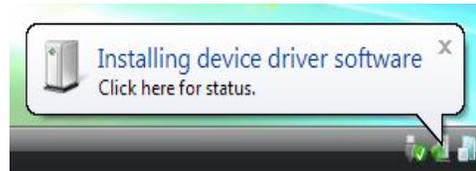


Figure 2.1 – Found New Hardware

Once the new hardware detection is complete, Windows will prompt you to begin the initialization process.

- Windows users will see an AutoPlay window similar to the one in **Figure 2.2**.
2. Select the option 'Run IronKey.exe'.

If Windows does not AutoPlay, you can browse to the CD-ROM partition (**Figure 2.3**) and manually execute the IronKey program. This will also start the initialization process.

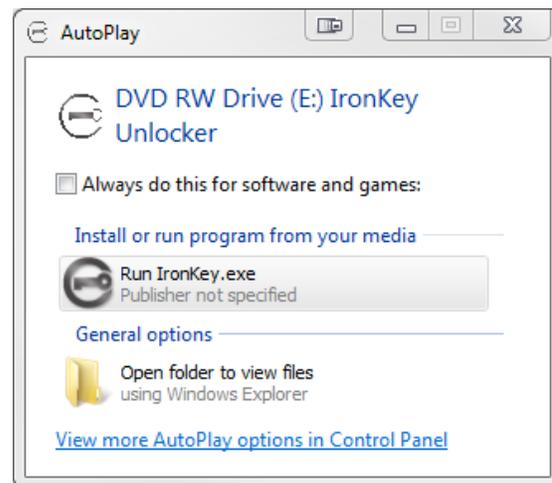


Figure 2.2 – AutoPlay Window

(Note: Menu options in the AutoPlay window may vary depending on what programs are currently installed on your computer. AutoRun will start the initialization process automatically.)

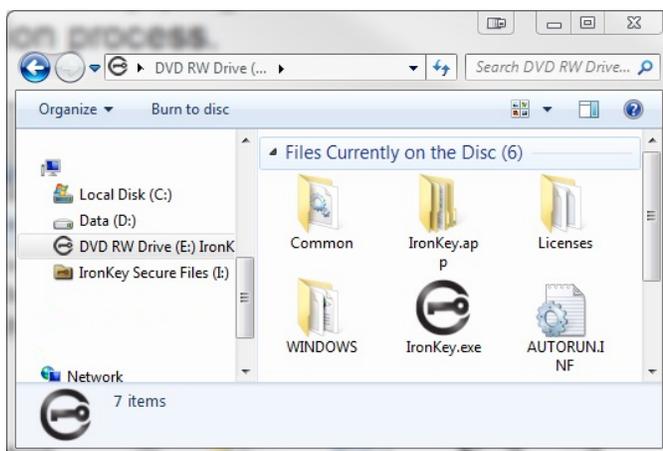


Figure 2.3 – D300M Contents

SETTING UP THE DEVICE (Mac OS's)

Insert the D300M into an available USB port on your notebook or desktop and wait for the Mac operating system to detect it. When it does, you will see a IRONKEY volume appear on the desktop, as seen in **Figure 3.1**.



Figure 3.1 – IRONKEY

1. Double-click the IRONKEY CD-ROM icon.
2. Look for IronKey.app found in the window displayed in **Figure 3.2**.
3. Double-click the Ironkey.app found in the window displayed in **Figure 3.3**. This will start the initialization process.

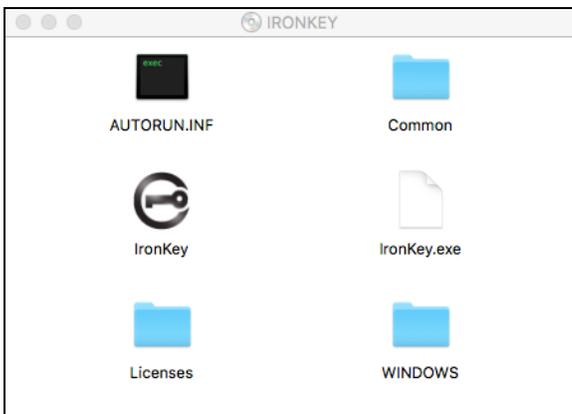


Figure 3.2 – D300M Contents

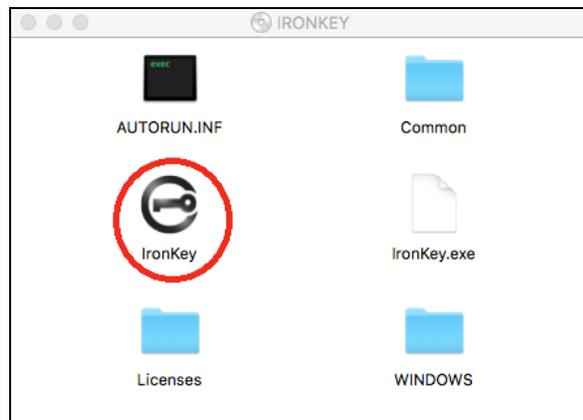


Figure 3.3 – D300M Application

Continue initialization on next page for both Windows and Mac OS's.

DEVICE INITIALIZATION/ACTIVATION

1. Type or paste the Activation Code. You should have received the code in an email message sent from your EMS Administrator. and click 'Next' (**Figure 4.1.**)

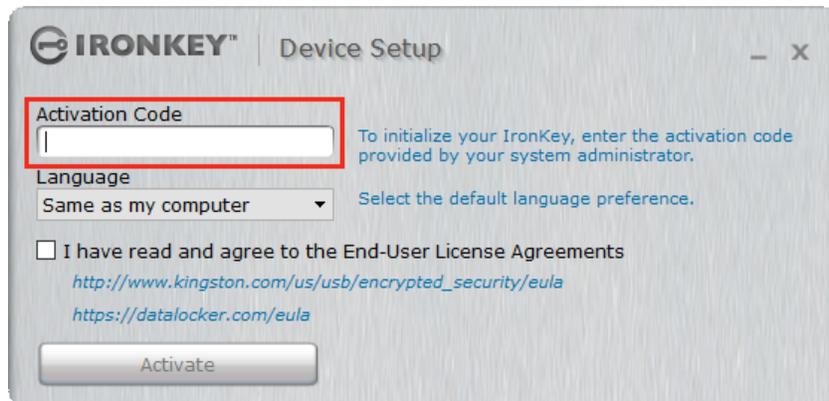


Figure 4.1 – Activation Code

2. Select the default language preference from the drop-down menu. By default IronKey software will use the same language as your computer's operating system. Continue to next step. (**Figure 4.2.**)



Figure 4.2 – Language Select

3. Review the license agreement and click 'Activate' **Figure 4.3.**

(Note: You must accept the license agreement before continuing; otherwise the 'Activate' button will remain disabled.)



Figure 4.3 – License Agreement

4. Create a password to protect your data on the D300M. Enter it in the 'Password' field, then re-enter it in the 'Confirm' field, as seen below in (**Figure 4.4**). Your password is case-sensitive and must comply with the password policy set by the administrator. Passwords must contain 8 characters or more (including spaces). Click 'Continue' and go to next step.



Figure 4.4 – Password Setup

5. You will be prompted to check your email. This is the email used when the Admin created the user account on IronKey™ EMS. Before continuing go to the your email and please follow the instructions. Once you have finished the email's instructions, click 'OK'. **Figure 4.5**

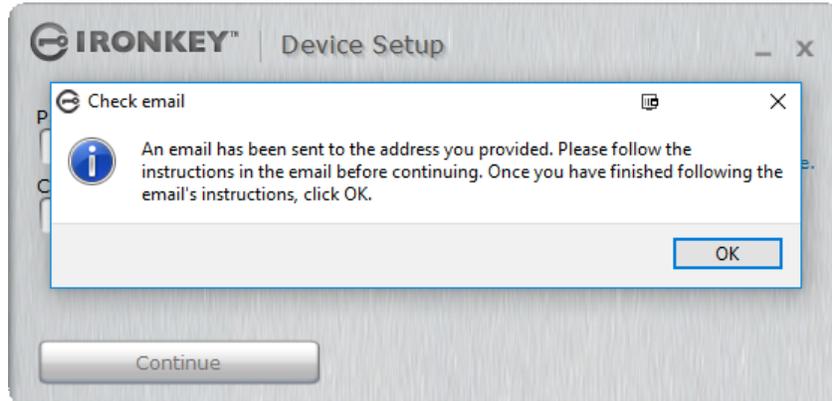


Figure 4.5 – Check Email

Device initialization\activation process is now complete.

USING MY DEVICE

Once the D300M has been initialized, you can access the secure data partition and utilize the device options by logging into the device with your password. To do so, follow these steps:

1. Insert the D300M into a USB port on your notebook or desktop.
 - Windows OS's - Run Ironkey.exe (Figure 2.3 on page 3)
 - Mac OS's - Run IronKey App (Figure 3.3 page 4)
2. Input Password (created on Figure 4.4 on page 6) **Figure 5.1**

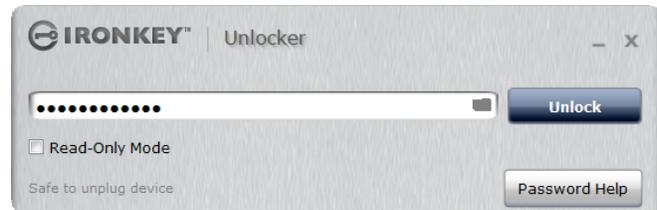


Figure 5.1 – Login Window

- Once you've typed your password, click the 'Unlock' button to continue.
- If the correct password is entered, the D300M will unlock and you can begin using the device.

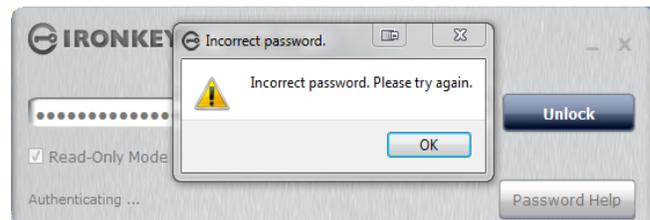


Figure 5.2 - Incorrect Password

- If an incorrect password is entered, an error message will appear stating '*Incorrect Password. Please try again.*'. **Figure 5.2**

(NOTE: During the login process, if a bad password is entered, you will be given another opportunity to enter the correct password; however, there is a built-in security feature that tracks the number of failed login attempts. If this number reaches the pre-configured value of 10 failed attempts, the D300M require a device reset of the secure data partition prior to next use. For more details on this feature, see 'Reset Device' on page 12.)*

3. You may unlock the secure data partition in read-only mode, sometimes referred to as "write-protect mode", by selecting the checkbox labeled 'Read-Only Mode' prior to logging into the device. Once authenticated under read-only, you will be allowed to open or view content on the D300M, but not update, change, or erase content while in this mode. *(Note: Read-only mode will also prevent the format option, the 'Reformat Secure Volume' will be grayed out.'*

If you are currently logged in under read-only mode and wish to unlock the device with full read/write access to the secure data partition, you must Lock D300M (**see #4 on Figure 6.1 next page**) and log back in, leaving the 'Read-Only Mode' checkbox unchecked during authentication.

** Once you authenticate to the device successfully, the failed login counter will be reset.*

DEVICE CONTROL PANEL (FEATURES)

CONTROL PANEL (APPLICATIONS) *Figure 6.1*

1. **Applications** - Opens Application list of Control Panel (current view)
2. **Files** - Opens Windows Explorer (PC) or Finder (Mac) for D300M's Secured Partition
3. **Settings** - Opens Control Panel's Settings
4. **Lock** - Locks D300M's Secured Partition
5. **Capacity Meter** - Shows available disk space of the Secured Partition

D300M Control Panel

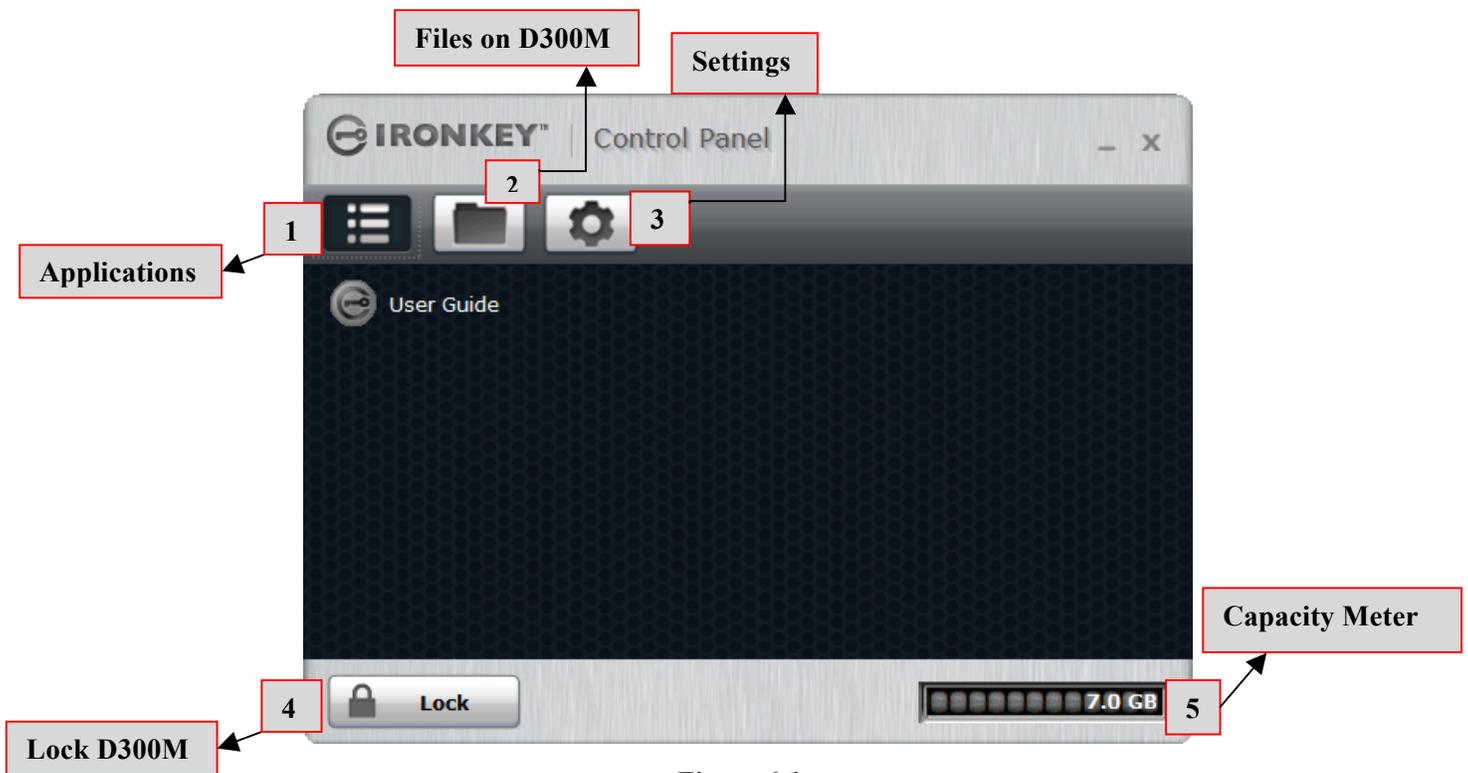


Figure 6.1

CONTROL PANEL (SETTINGS)

1. **Tools** - Opens Control Panel Tools Options (*Figure 6.2*)
 - **Check for Updates** (default = Automatically check for updates)
 - **Reformats the Secure Volume***

***Warning: All data will be lost on Secure Volume. Backup data before doing a reformat.**



Figure 6.2 Control Panel - Settings - Tools

2. **Password** - Opens Control Panel Password Options (*Figure 6.3*)
 - **If I forgot my password...** (default = Enabled Password Reset)
 - **Change Password** (based on password policy set by IronKey EMS Admin)



Figure 6.3 Control Panel - Settings - Password

3. Preferences - Opens Control Panel Preferences Options (*Figure 6.4*)

- Change Language used for D300M (default = Same as my computer)
- Unlock Message can be used or changed on D300M Unlock screen (default = disallowed)

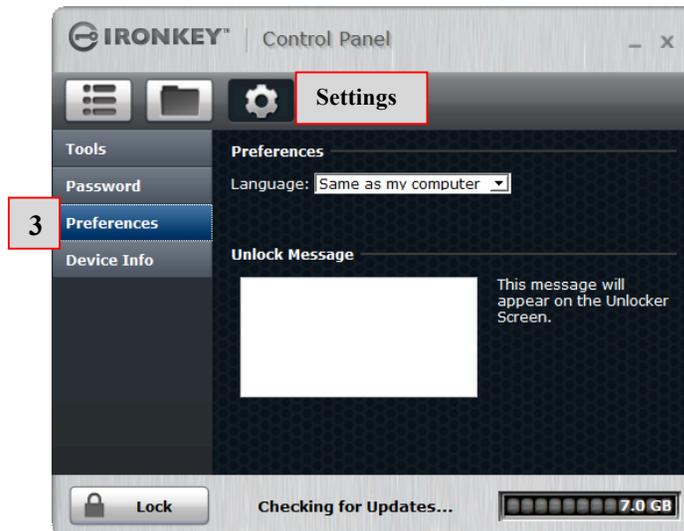


Figure 6.4 Control Panel - Settings - Preferences

4. Device Info - Opens Control Panel Device Info Options (*Figure 6.5*)

- Copy will copy the data for About This Device to the clipboard and can be pasted into an email or text editor
- Visit Website launches browser to Kingston's Secure USB Homepage
- Legal Notices launches browser to the D300M Software License Agreement website
- Certifications launches open browser to the D300M certifications website



(Figure 6.5) Control Panel - Settings - Device Info

HELP AND TROUBLESHOOTING

RESET DEVICE

The D300M includes a security feature that prevents unauthorized access to the data partition once a maximum number of **consecutive** failed login attempts (*MaxNoA* for short) has been made; the default “out-of-box” configuration has a pre-configured value of 10 number of attempts. **(NOTE: Based on default policy.)**

The ‘lock-out’ counter tracks each failed login and gets reset one of two ways: **1)** A successful login prior to reaching *MaxNoA* or **2)** reaching *MaxNoA* and performing a device format. ***(NOTE: Method (2) all data is lost.)**

If an incorrect password is entered, an error message will be displayed. See **Figure 7.1**.

ON the 2nd incorrect password attempt you will see an additional error message indicating you have 8 attempts left before reaching *MaxNoA* (which is set to 10 by default.) You will also see an option for Reset Device. See **Figure 7.2**.

You can choose to Reset Device at this point if you: 1) want to put the drive to an Out-of-Box state or 2) You know you won't remember the password.*

After a 10th incorrect password attempt, the D300M will permanently block the data partition and require a device reset prior to next use. This means that **all data stored on the D300M will be lost** and you will need to reactivate the D300M with a new activation code from the EMS Admin.

This security measure limits someone (who does not have your password) from attempting countless login attempts and gaining access to your sensitive data.

***Note: A device reset will erase ALL of the information stored on the D300M's secure data partition.**



Figure 7.1 – Login Failure

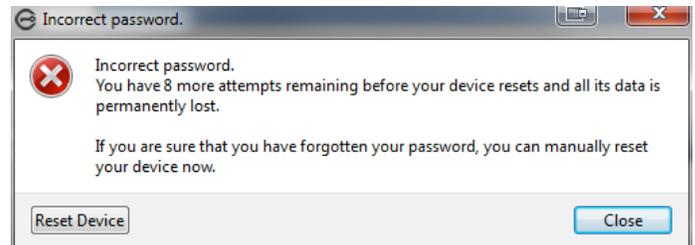


Figure 7.2 – 2nd Incorrect Password

USING PASSWORD HELP

To reset your password:

1. Plug in D300M and run the IronKey.exe (Windows OS's) and Ironkey.app (Mac OS's).
2. Click Password Help. **Figure 8.1**

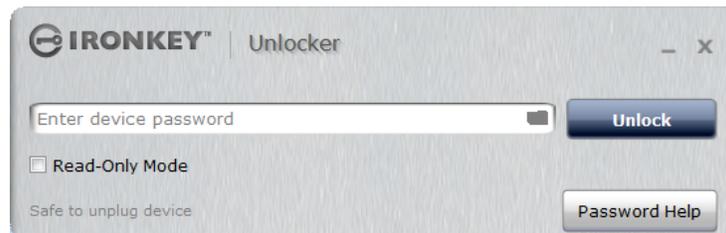


Figure 8.1

3. At the Password Help prompt, click on the Reset Password. **Figure 8.2**

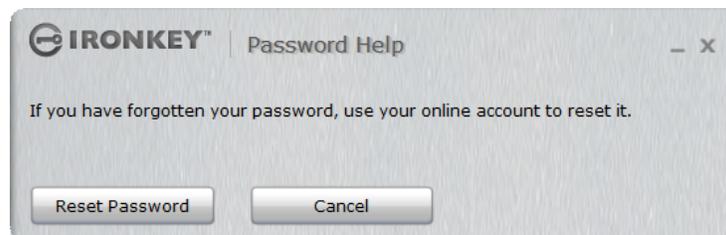


Figure 8.2

4. After you complete the instructions in the email message, enter code and Click Continue. **Figure 8.3**



Figure 8.3

5. Type your new password and confirm the password in the fields provided and Click Change Password. **(Figure 8.4)** This completes the process of changing your password.



Figure 8.4

DRIVE LETTER CONFLICTS (Windows Operating Systems)

As mentioned in the ‘*System Requirements*’ section of this manual (on page 2), the D300M requires two consecutive drive letters AFTER the last physical disk that appears before the ‘gap’ in drive letter assignments (see **Figure 9.1.**) This does NOT pertain to network shares because they are specific to user-profiles and not the system hardware profile itself, thus appearing available to the OS.

What this means is, Windows may assign the D300M a drive letter that’s already in use by a network share or Universal Naming Convention (UNC) path, causing a drive letter conflict. If this happens, please consult your administrator or helpdesk department on changing drive letter assignments in Windows Disk Management (administrator privileges required.)

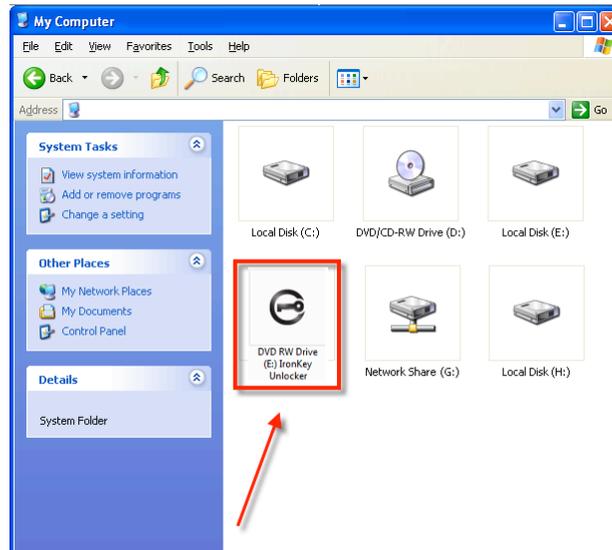


Figure 9.1 – My Computer

In this example, the D300M uses drive F:, which is the first available drive letter after drive E: (the last physical disk before the drive letter gap.) Because letter G: is a network share and not part of the hardware profile, the D300M may attempt to use it as its second drive letter, causing a conflict.

If there are no network shares on your system and the D300M still won’t load, it is possible that a card reader, removable disk, or other previously-installed device is holding on to a drive-letter assignment and still causing a conflict.

Please note that Drive Letter Management, or DLM, has improved significantly in Windows Vista, 7, 8/8.1 and 10 so you may not come across this issue, but if you are unable to resolve the conflict, please contact Kingston’s Technical Support Department for further assistance.

ERROR MESSAGES

Unable to create file – This error message will appear when attempting to **CREATE** a file or folder **ON** the secure data partition while logged in under read-only mode.



Figure 11.1 – Unable to Create File Error

Error Copying File or Folder – This error message will appear when attempting to **COPY** a file or folder **TO** the secure data partition while logged in under read-only mode.



Figure 11.2 – Error Copying File or Folder Error

Error Deleting File or Folder – This error message will appear when attempting to **DELETE** a file or folder **FROM** the secure data partition while logged in under read-only mode.



Figure 11.3 – Error Deleting File or Folder Error

If you are ever logged in under read-only mode and wish to unlock the device with full read/write access to the secure data partition, you must 'Lock' D300M and log back in, leaving the 'Read-Only Mode' checkbox unchecked prior to login.