Learn About BitLocker (Encryption for Windows)
Stephanie Obodda - 2017-02-16 - 0 Comments - in Encryption

- What is BitLocker?
- Who should be using Bitlocker?
- How can I obtain it?
- How do I use BitLocker to encrypt my laptop?
- Where can I find written documentation?
- What should I know about decryption?
- What restrictions are there when traveling out of the country with an encrypted laptop?
- Resources

Q. What is BitLocker?
A. BitLocker Drive Encryption is an integral security feature for Windows computers. It provides protection for your computer's operating system as well as the data stored it, ensuring that the data remains encrypted even if the computer is tampered with when the operating system is not running. This helps protect against "offline attacks," those made by disabling or circumventing the installed operating system, or made by physically removing the hard drive to attack the data separately.

Q. Who should be using Bitlocker?
A. ISG recommends that faculty and staff enable BitLocker if they use laptops containing Brown Restricted Information (especially frequent travelers). Use Identity Finder to determine the presence of BRI. If detected, either remove it, or if necessary, encrypt it.

Q. How can I obtain it?
A. BitLocker is built into the Windows operating system, but is not enabled by default. Your IT Support Professional will determine if you need BitLocker enabled and perform the necessary steps.

Q. How do I use BitLocker to encrypt my laptop?
A. Your IT Support Professional will enable BitLocker.
Q. Where can I find written documentation?
A. Microsoft provides an overview and guide for using BitLocker with Windows 7, 8.1, 10 and 10 Mobile.

Q. What should I know about decryption?
A. In the event that you feel your computer needs to be decrypted contact your IT Support Professional, or if none, the IT Service Center. Note that the decryption process will take about the same length of time as encryption did.

Q. I have a computer encrypted but when I start it up, the following screen appears:

A. Bitlocker has detected that something with your computer hardware has changed. This is a security feature designed to protect your data. For example, someone could have stolen your computer and is attempting to bypass the normal startup sequence. Follow the step below to obtain a recovery password. Please note, you will need access to another device with a web browser.

1. Press any key to continue, the next screen will be similar to this.
3. When prompted, enter your Brown UserID and Password.
4. Check the box next to "I have read and understand the above notice".
5. At this screen, enter the first 8 digits of "Password ID" from the screen above from your computer:

   Brown University

   Get a BitLocker Recovery Key

   Use this page if you are locked out of Windows by BitLocker and need to get a BitLocker Recovery Key to regain access to Windows.

   NOTE: For security reasons, your session will expire after 5 minute(s) of inactivity. You will need to re-enter your information into the form on this page.

   Enter a BitLocker Key ID

   This 32-digit code should be displayed on the BitLocker recovery screen on your computer. Enter a minimum of 8 characters.

   Recovery Key ID

   Reason

   Get Key

   Your BitLocker Recovery Key

   Enter this 48-digit code into the BitLocker recovery screen on your computer.

6. Finally, enter the 48-digit code into the recovery screen on your computer.
Q. What restrictions are there when traveling out of the country with an encrypted laptop?

A. U.S. federal regulations control the export of "encryption commodities, software and technology" (see Code of Federal Regulations, Title 15, Section 740.17). There are, however, license exceptions that allow you to take encrypted laptops with them, provided that they return within the year and "retain effective control and ownership." This coverage is global except for a handful embargoed and sanctioned countries designated by the U.S. government. Travel to any of these countries requires that you remove any encryption technology from your laptop before entering it.

In addition, as some countries ban or severely regulate the use of encryption, you should check country-specific information before traveling with an encrypted laptop. Following is a partial list of those countries. Check the U.S. State Department website before traveling to verify that the information is still current. In addition, any faculty, post-docs, graduate students and PI's should check-in with OVPR, Insurance and Risk, and the Director of Information Technology Security before travelling overseas.

- Burma (you must apply for a license)
- Belarus (import and export of cryptography is restricted; you must apply for a license from the Ministry of Foreign Affairs or the State Centre for Information Security or the State Security Agency before entry)
- China (you must apply for a permit from the Beijing Office of State Encryption Administrative Bureau; travelers should also refrain from purchasing a replacement laptop when visiting China. It is known for intellectual espionage and such laptops could contain malware to steal content added to it.)
- Hungary (import controls)
- Iran (strict domestic controls)
- Israel (personal-use exemption – must present the password when requested to prove the encrypted data is personal)
- Morocco (stringent import, export and domestic controls enacted)
- Russia (you must apply for a license)
- Saudi Arabia (encryption is generally banned)
- Tunisia (import of cryptography is restricted)
- Ukraine (stringent import, export and domestic controls)

Resources

- Turn on Device Encryption (Windows 10)
- Help protect your files using BitLocker Drive Encryption: Windows 7 | Windows 8 | Windows 10

Internal links about traveling:
• Brown’s Travel Portal and Export Controls guidelines
• International Travel Information for all Brown University Travelers
• Export Controls at Brown | Brown’s Export Control Policy

Note: For questions or further information related to export controls or international research administration, please contact Juliane_Blyth@brown.edu, Associate Director of Research Operations at (401) 863-3295.

External links about traveling:

• Encryption FAQs (Bureau of Industry & Security, BIS)
• EAR Controls for Items That Use Encryption (Bureau of Industry & Security, BIS)
• Cornell University - Travel Internationally with Technology
• FBI - Safety and Security Guidance for Traveling Abroad
• Department of State - Travel Alerts and Warnings
• Department of Homeland Security - "Know Before You Go" Resources
• Department of State - Websites of US Embassies Consulates, and Diplomatic Missions
• Department of State - "Smart Traveler Enrollment Program"