

Announcement: Remediating CrowdStrike Falcon Issue

Addressing CrowdStrike Falcon Content Update Interruption and for Windows Hosts

Unlocking Drive for CrowdStrike Remediation

We are aware of the current issue with the CrowdStrike Falcon Content Update, which has rendered numerous Windows devices inaccessible worldwide. We understand the impact this has on your daily operations and are committed to providing immediate assistance.

For more on this issue, please read CrowdStrike's blog here -

<https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/>

Note that with WinMagic's SecureDoc, Your Data Remains Secure

While CrowdStrike is actively working on a resolution, we want to assure you that your data remains secure with SecureDoc encryption.

Step 1: Follow the Instructions Provided by CrowdStrike as their latest instructions on remediation should not be affected by SecureDoc or encrypted drives

Step 2: If CrowdStrike remediation is unsuccessful with Encrypted Drives: Steps to Unlock Encrypted Drives

If you need to unlock the encrypted drive to access your data or for CrowdStrike remediation steps, you can do so by booting into WinPE and by following the steps below depending on your encryption type (Software, Hardware or Bitlocker).

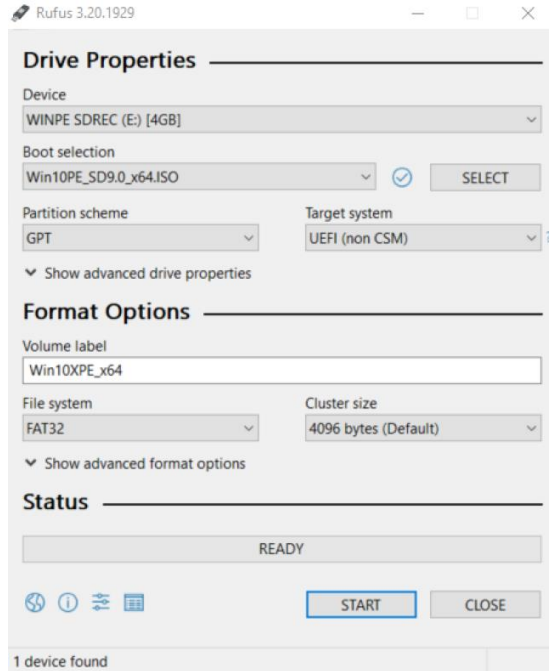
You can verify your encryption type in your SES console by selecting a device and looking under the "Encryption Type" column.

How to create a bootable WinPE USB:

1. Download Rufus software: <http://rufus.akeo.ie/>
2. Download WinPE 9.1 ISO from here:
<https://fileshare.winmagic.com/link/zgmliatMkUry7TOe3G8eo4>
3. Configure Rufus as shown in the screenshot

a. Either set to GPT for UEFI or MBR Partition for UEFI

b. Format USB to FAT32

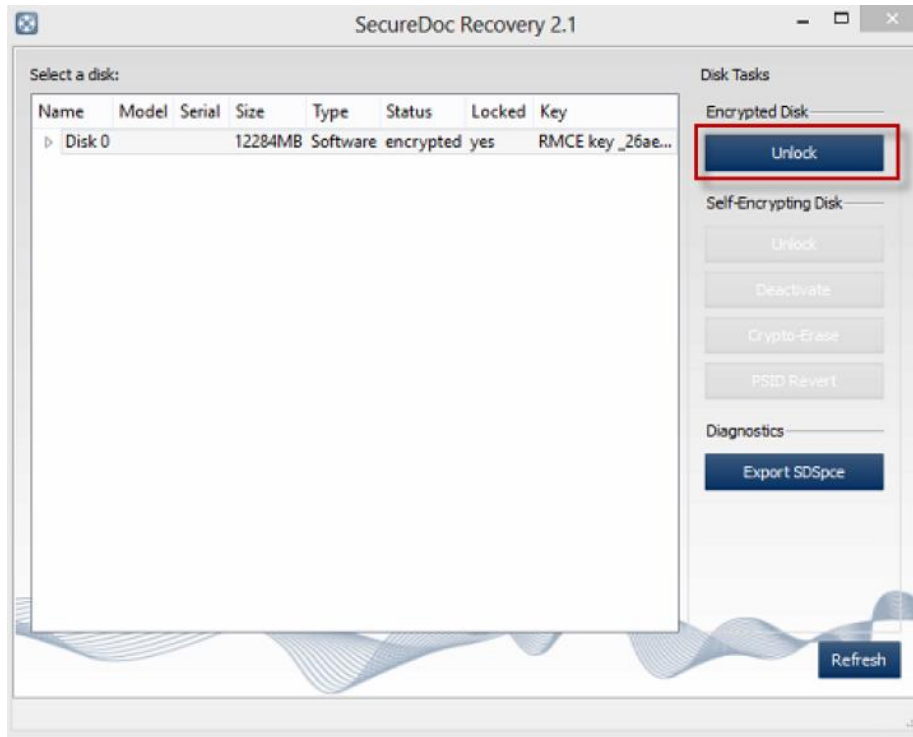


The screenshot shows the Rufus 3.20.1929 application window. The 'Drive Properties' section is active, showing the device 'WINPE SDREC (E:) [4GB]'. The 'Boot selection' is set to 'Win10PE_SD9.0_x64.ISO' with a 'SELECT' button. The 'Partition scheme' is set to 'GPT' and the 'Target system' is set to 'UEFI (non CSM)'. There is a 'Show advanced drive properties' checkbox. The 'Format Options' section shows the 'Volume label' as 'Win10XPE_x64', the 'File system' as 'FAT32', and the 'Cluster size' as '4096 bytes (Default)'. There is a 'Show advanced format options' checkbox. The 'Status' section shows a progress bar at 'READY'. At the bottom, there are icons for help, info, settings, and a list, along with 'START' and 'CLOSE' buttons. A status bar at the very bottom indicates '1 device found'.

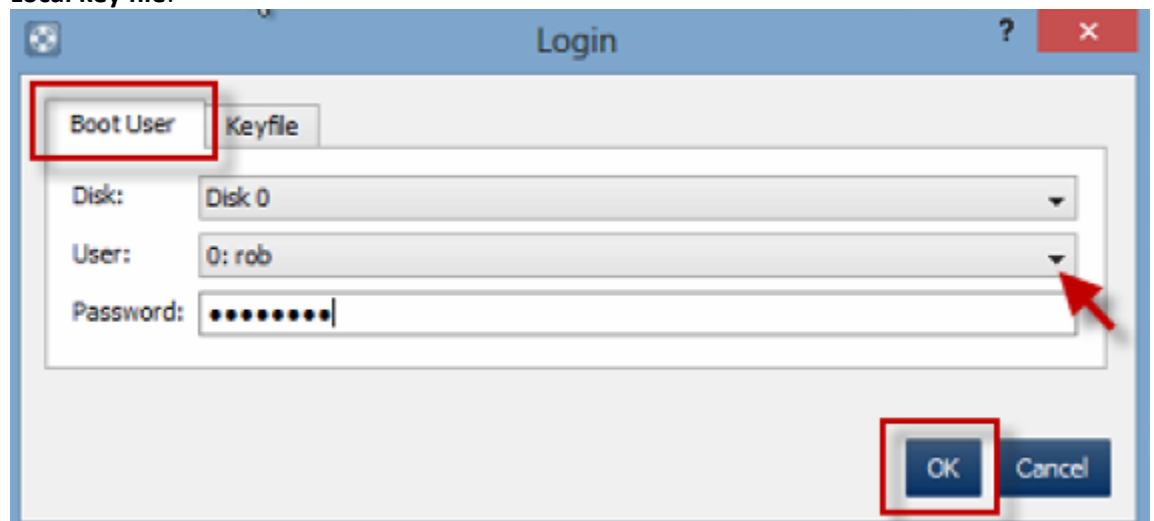
4. Select the ISO image and hit Start.
5. Power off/on the device, open the boot menu and boot to the USB.
6. Launch SDRcovery, which is located on the Desktop.

Unlock Software Encrypted Drive

1. Select the drive and click 'Unlock'.



2. You will be presented with a Window to unlock the drive by the boot user (local key file) password or by an external key file.
 - a. **Local key file:**

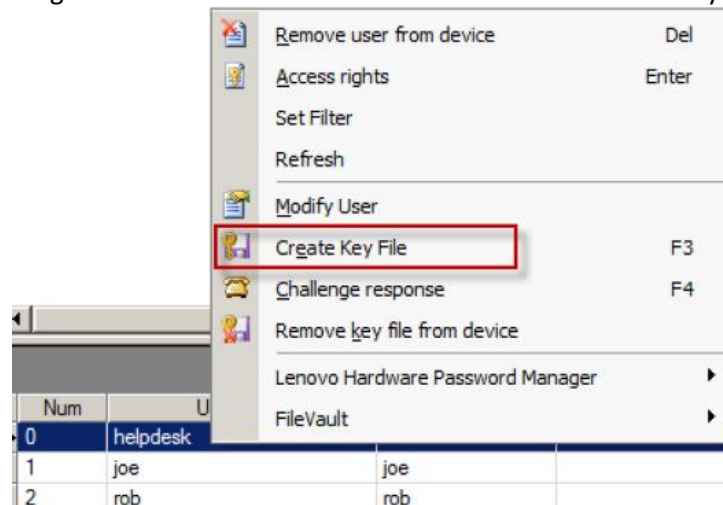


- b. **External key file:** If the password to local keyfile is unknown, then a key file from SES is required for the target drive.
 - First identify and highlight the target computer in SES.
 - Select a valid account under the target device.

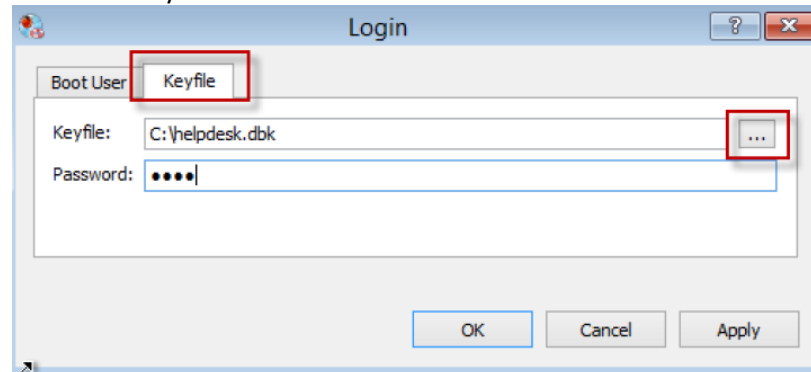
6	WIN-G23D4U821IK	VMware, Inc.	VMware-56 4d 28	11/20/2012 8:53:48 PM	11/20/2012 7:51:34 PM	Not activated	V
---	-----------------	--------------	-----------------	-----------------------	-----------------------	---------------	---

Users having access to the device 'WIN							
Num	User ID	First name	Last name	email	KeyFile	Lenovo HPM Us	
0	helpdesk				Present		
1	joe	joe			Present		
2	rob	rob			Present		

- Right-click on the selected account and choose Create Key File:



- Save the key file to a USB and use it to unlock the disk in SDRecovery:

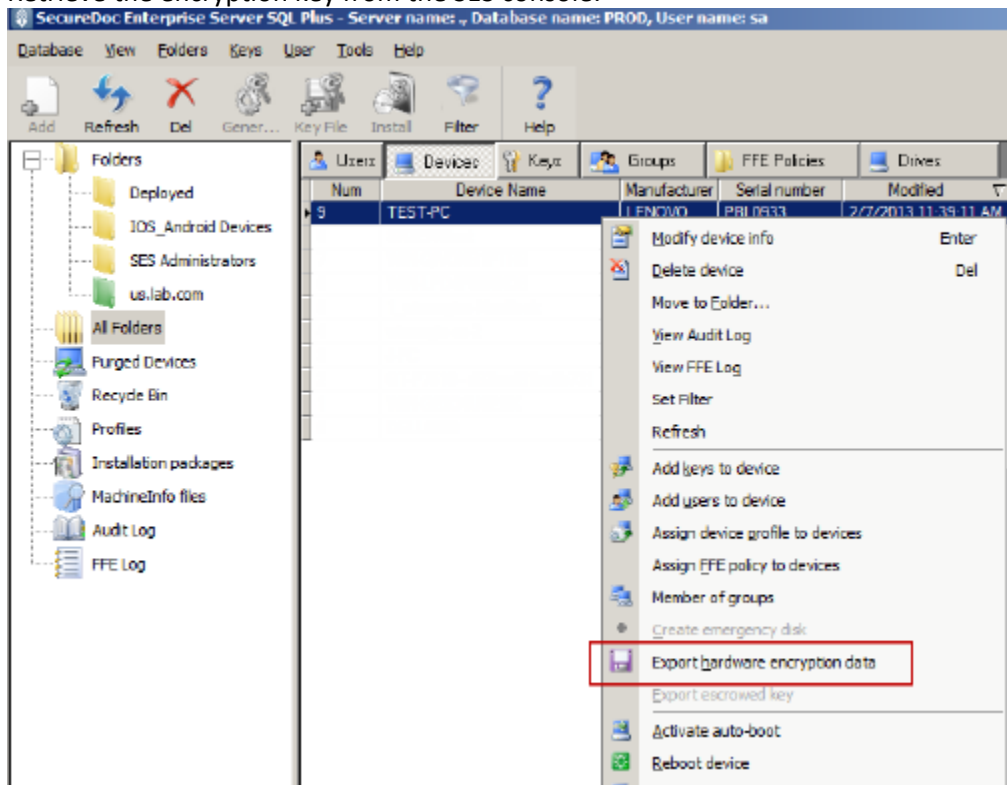


3. A prompt should now appear saying the drive was unlocked.

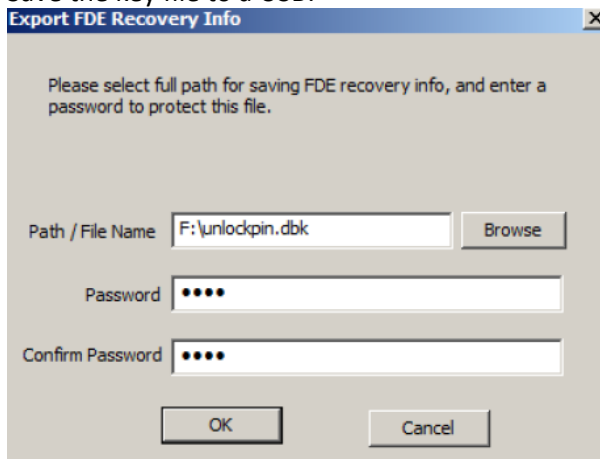


Unlock Hardware Encrypted Drive

1. Retrieve the encryption key from the SES console:



2. Save the key file to a USB:



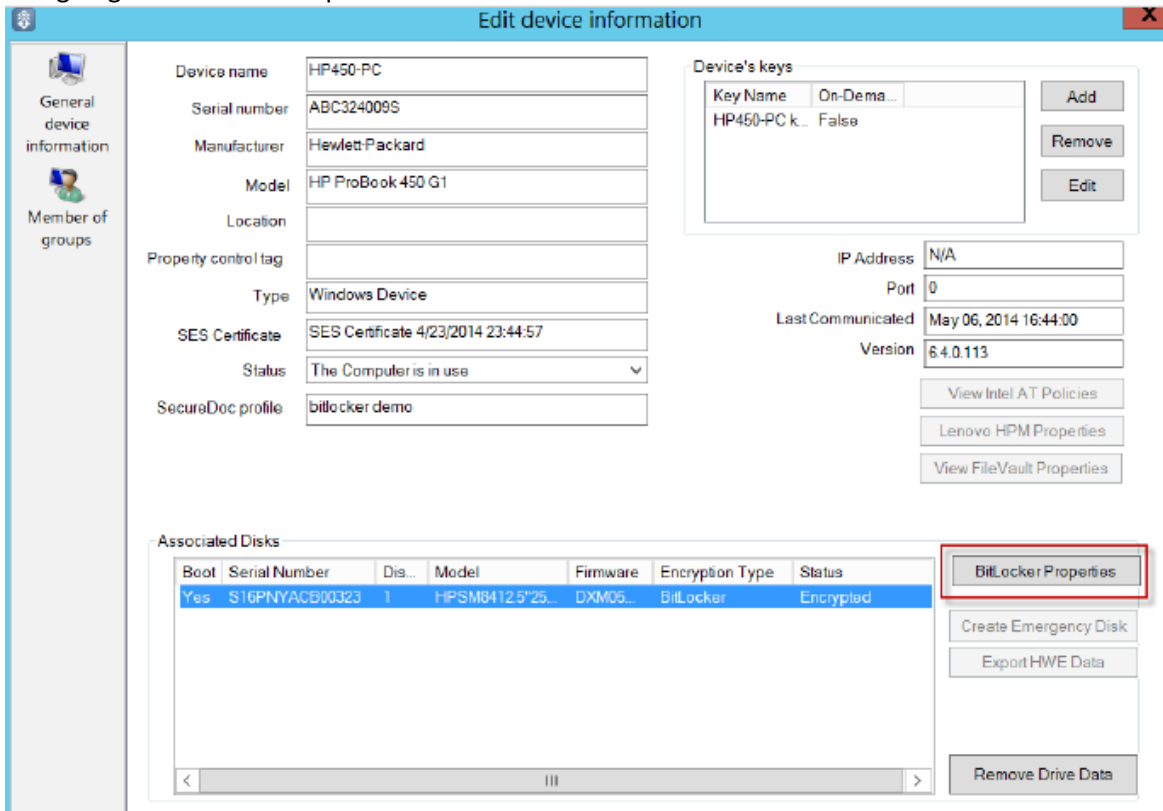
3. In SDR Recovery, select the drive and click "Unlock". You will be presented with a screen to log into the key file you exported in the previous step.

4. A prompt should now appear saying the drive was unlocked.



Unlock Bitlocker Encrypted Drive

1. Retrieve the Bitlocker recovery key from the SES console by double clicking on the target device and going to "Bitlocker Properties":



Edit device information

General device information

Member of groups

Device name: HP450-PC

Serial number: ABC324009S

Manufacturer: Hewlett-Packard

Model: HP ProBook 450 G1

Location:

Property control tag:

Type: Windows Device

SES Certificate: SES Certificate 4/23/2014 23:44:57

Status: The Computer is in use

SecurDoc profile: bitlocker demo

Device's keys

Key Name	On-Dema...
HP450-PC k...	False

IP Address: N/A

Port: 0

Last Communicated: May 06, 2014 16:44:00

Version: 6.4.0.113

View Intel AT Policies

Lenovo HPM Properties

View FileVault Properties

Associated Disks

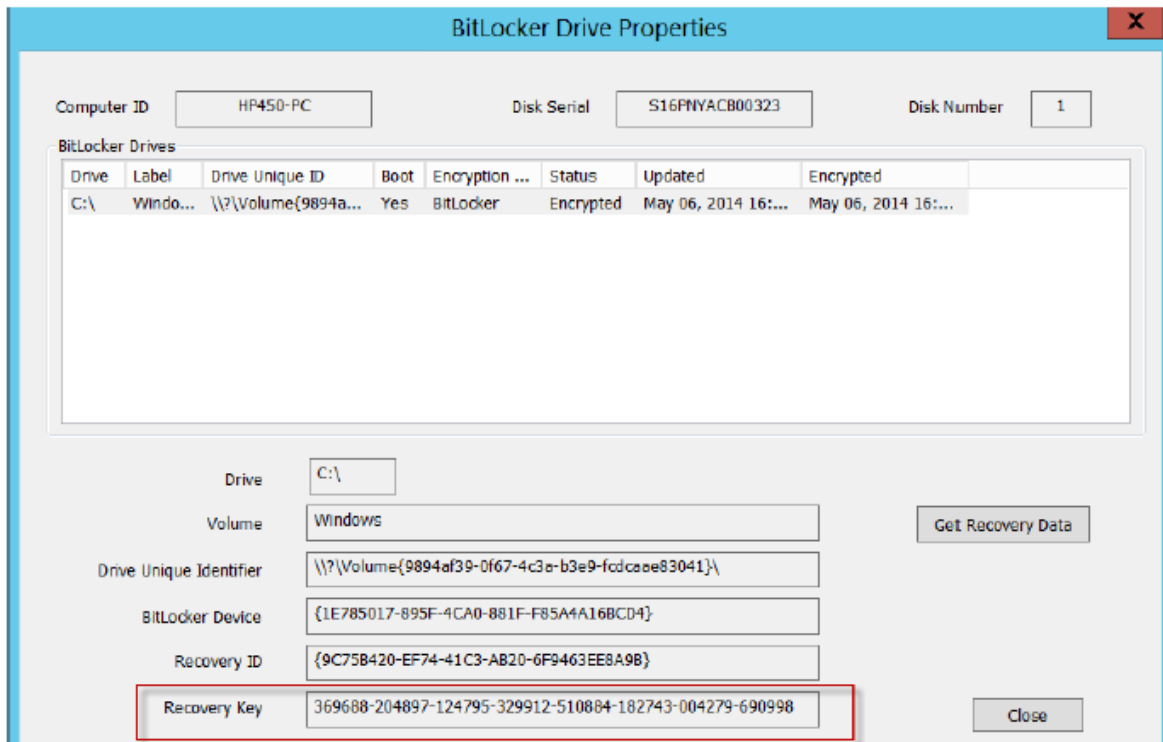
Boot	Serial Number	Dis...	Model	Firmware	Encryption Type	Status
Yes	S16PNYACB00323	1	HP5M84125"25...	DXM05...	BitLocker	Encrypted

BitLocker Properties

Create Emergency Disk

Export HWE Data

Remove Drive Data



BitLocker Drive Properties

Computer ID: HP450-PC

Disk Serial: S16PNYACB00323

Disk Number: 1

BitLocker Drives

Drive	Label	Drive Unique ID	Boot	Encryption ...	Status	Updated	Encrypted
C:\	Windo...	\\?\Volume{9894a...	Yes	BitLocker	Encrypted	May 06, 2014 16:...	May 06, 2014 16:...

Drive: C:\

Volume: Windows

Drive Unique Identifier: \\?\Volume{9894af39-0f67-4c3e-b3e9-fdcdae83041}\

BitLocker Device: {1E785017-895F-4CA0-881F-F85A4A16BCD4}

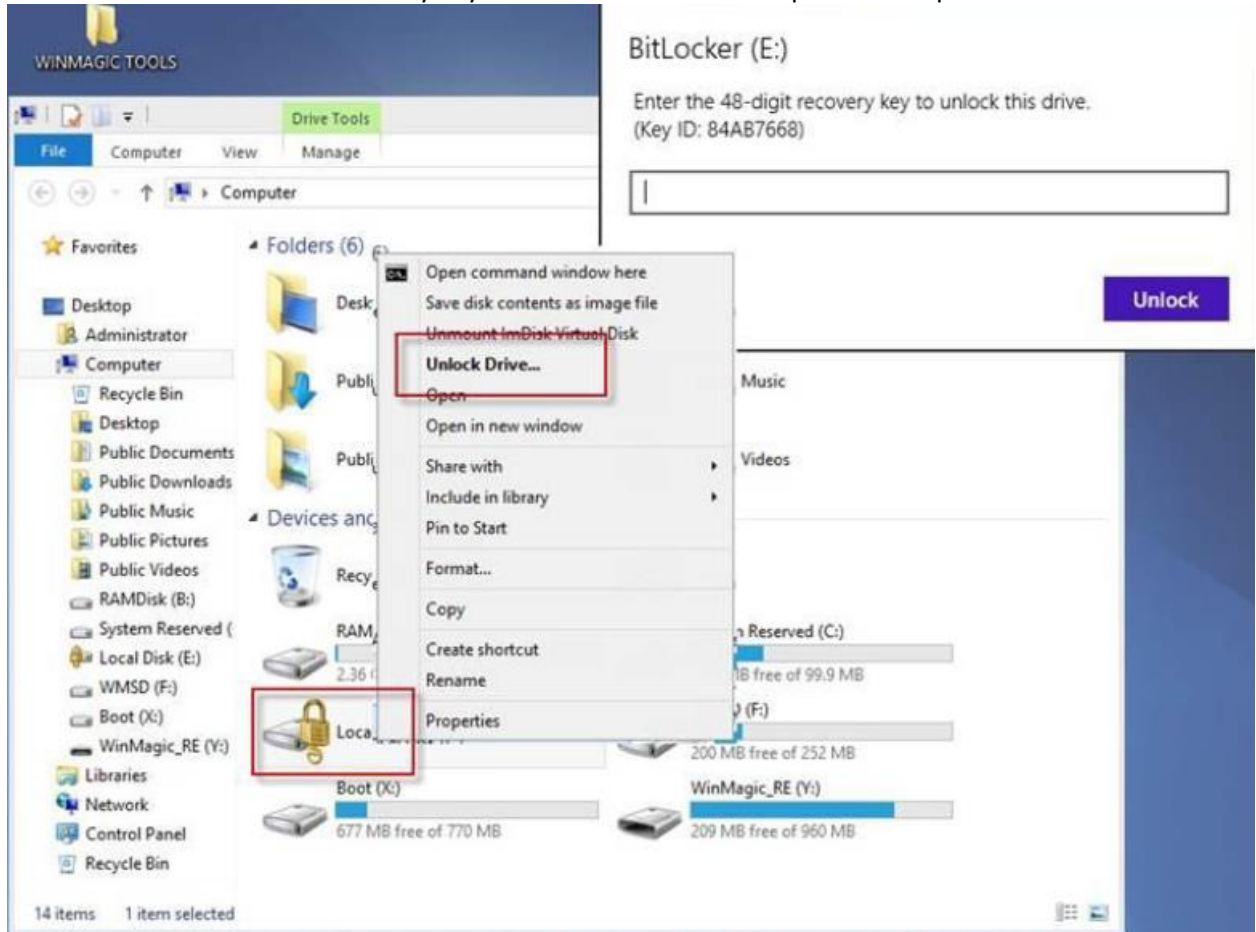
Recovery ID: {9C75B420-EF74-41C3-AB20-6F9463EE8A9B}

Recovery Key: 369688-204897-124795-329912-510884-182743-004279-690998

Get Recovery Data

Close

2. While booted into WinPE, launch Windows Explorer and right click the encrypted drive > “Unlock Drive” > Enter the recovery key that was extracted in the previous step:



3. The drive should now be unlocked.