

# Security Removable Media Manager

# Encrypted Cd/Dvd/Blu-ray User Guide

Version 9.11.35.0 (March 2025) Protect your valuable data



#### © 2011 Squadra Technologies, LLC. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Squadra Technologies, LLC.

If you have any questions regarding your potential use of this material, contact:

Squadra Technologies, LLC 4201 State Route W Cleveland, Missouri 64734 USA www.squadratechnologies.com email: info@squadratechnologies.com

Refer to our Web site for regional and international office information.

#### TRADEMARKS

Squadra Technologies, secRMM are trademarks and registered trademarks of Squadra Technologies, LLC. Other trademarks and registered trademarks used in this guide are property of their respective owners.

#### Disclaimer

The information in this document is provided in connection with Squadra Technologies products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Squadra Technologies products. EXCEPT AS SET FORTH IN Squadra Technologies's TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, Squadra Technologies ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL Squadra Technologies BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF Squadra Technologies HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Squadra Technologies makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Squadra Technologies does not make any commitment to update the information contained in this document.

Squadra Technologies Administrator Guide Created - March 2011

# Contents

SECRMM INTRODUCTION	4
SECRMM 'ENCRYPTED DISC' INTRODUCTION	4
ENCRYPTION INFORMATION	5
PREREQUISITES	6
CREATE AN ENCRYPTED DISC	6
Preapproval (two man policy)	15
UNLOCK AN ENCRYPTED DISC	19
UNMOUNT AN ENCRYPTED DISC	24
USING AN ENCRYPTED DISC WHERE SECRMM IS NOT INSTALLED	26
Using the secRMM provided programs on the disc	26 27
Unlock an encrypted disc	27
Misleading Windows Explorer pop-up error message Unmount an encrypted disc	31 32
ADMINISTRATOR/ADVANCED SECTION	33
PowerShell	
Overriding Enable-BitLocker	
Using the PowerShell scripts without a GUI	35
DEBUGGING	35
Debug file locations	38
TROUBLESHOOTING	40
KNOWN ISSUES	42
CONTACTING SQUADRA TECHNOLOGIES SUPPORT	47
ABOUT SQUADRA TECHNOLOGIES, LLC.	47

#### secRMM Introduction

Squadra Technologies security Removable Media Manager (secRMM) software is Windows security software that runs on your company's workstations and servers. secRMM manages and monitors removable media. In this context, Removable media is defined as external hard disks, USB (flash) drives, smart phones, tablets, SD-Cards, CD-ROM, DVD and Blu-ray. Generally, any storage device that supports Microsoft plug-and-play will be managed and monitored by secRMM. Such devices typically use the computers Universal Serial Bus (USB) ports to connect to the computer. Removable media devices are popular because they are very convenient when you want to copy files around or backup data. secRMM allows you to track all write activity to the removable media devices in your computer environment as well as giving you the ability to

Computer Management (Local)	Computer Configuration		Actions
Computer wanagement (Uccal) C System Tools C System Tools C System Cools C	Lonputer Lonfugaration Name AlswalttackenChip Alawad Steatorise Book Office Macroso Charlows Book Office Macroso Book Office Mac	Value 01/15/2024 09 20:58 on SCCMIR2 9.11.28.0	Actions seeRMM SafeCopy Approver SeeRMM Charts SeeRMM Charts Device Tracker SeeRMM License SeeRMM License SeeRMM Configuration Vew Help

control (or authorize) who can write to the removable media devices.

This document will reference the term "CD/DVD/Blu-ray discs" as just "discs" so the documentation is not cluttered with this long term.

# secRMM 'encrypted disc' Introduction

When secRMM is installed on a Windows computer, a program named secRMMSafeCopy gets installed. secRMMSafeCopy is installed into "C:\Program Files\secRMM\UserUtils\secRMMSafeCopy.exe".

File     Home     Share     View	App	Manage lication Tools	UserUtils			-		× ^ (?)
Pin to Quick access Copy Paste Paste sh Clipboard	th ortcut	Move Copy to * Copy	Delete Rename	New item • New folder New	Properties Open • Properties	Select all Select none Invert select Select	tion	
← → ~ ↑ 📴 > This PC > 05	(C:) >	Program Files	secRMM > Use	erUtils		~ Ō	Search Us.	
Music	^	Name		~	Date modified	Туре	й. Г	^
Pictures		19 secRM	MSafeConv.chm		3/1/2025 7:44 A	M Com	piled HTML	
Videos		secRMI	MSafeCopy.exe		3/1/2025 7:46 A	M Appl	lication	
L OS (C:)		SECKIWI	visarecopycontact	info.html	6/25/2018 5:43	PM Firef	ox HTML De	oc
D drive (D:)		😰 secRMI	MSafeSync.chm		3/1/2025 7:51 A	M Com	piled HTML	
DVD PW Drive (E-) 2025 02 28 12	21	( secRMI	MSafeSync.exe		3/1/2025 7:51 A	M Appl	lication	
0 0 0 KW DIVE (E.) 2023.02.20_13	51	SmartC	ardPinPrompt.cmc	i i	3/9/2020 5:34 P	M Wind	dows Comm	18
OVD RW Drive (E:) 2025.02.28_133	1	SmartC	ardPinPrompt.hta		1/23/2022 12:40	PM HTM	IL Applicatio	on in
<b>A</b> N. 4 1		SmartC	ardPinPrompt.ico		2/22/2020 3:05	PM Icon		
Network		SmartC	ardPinPrompt.log		3/1/2020 11:42	AM LOG	File	
W9		SmartC	ardPinPrompt.png		2/22/2020 3:10	PM PNG	File	~
	~	<		2				>

Note that the parent folder "C:\Program Files\secRMM" is not accessible unless you are logged in as an Administrator. If you do not have Administrator permissions on the Windows computer, you should contact your system Administrator and have them create a desktop short cut for you to be able to access secRMMSafeCopy. Alternatively, you must manually type the path into explorer (i.e. your must type C:\Program Files\secRMM\UserUtils and hit enter).

secRMMSafeCopy is the secRMM program that will let you perform the 3 encrypted disc functions:

- 1. Create
- 2. Unlock
- 3. Unmount

The encrypted disc functions that secRMMSafeCopy provides are meant to meet requirements for specific customers who need to create encrypted discs and have them be write-protected after the initial data is copied to them. The discs are then used in air-gapped/classified environments. If you are looking to create audio or ISO discs, you will need to look at other disc burning solutions on the market since secRMMSafeCopy will only burn encrypted data discs.

#### **Encryption information**

secRMMSafeCopy uses Microsoft BitLocker to create the encrypted discs. Using the Microsoft BitLocker technology was chosen because it is certified by the Federal Information Processing Standard (FIPS) Publication 140-2. FIPS 140-2 is a U.S. government computer security standard used to approve cryptographic (i.e. security) modules. secRMMSafeCopy first creates a Microsoft Virtual Hard Drive (VHD), then copies the data files (you want on the encrypted disc) to the VHD and then BitLocker encrypts the VHD using a password supplied by the end-user who is creating the disc. Using 3 very popular Microsoft technologies (VHD, BitLocker and PowerShell) to accomplish the encrypted disc gives you the most secure

solution with the capability to expand it and use it within your entire enterprise, even if secRMM is not installed.

## **Prerequisites**

- 1. Microsoft .Net 4.0 (or greater) Framework.
- 2. PowerShell 3.0 (or greater)

## **Create an encrypted disc**

Please follow the steps and screenshots in this section to create an encrypted disc using secRMMSafeCopy.

1. Start the secRMMSafeCopy program<sup>1</sup>

<sup>&</sup>lt;sup>1</sup> Consider disconnecting the external CD drive(s) before you start secRMMSafeCopy because it needs to read all the CD drive properties. If you have an external CD drive(s) connected when you start secRMMSafeCopy, it will appear to hang because it is reading the external CD drive properties which takes several seconds. Once the secRMMSafeCopy window opens, then attach the external CD drive(s).



2. If you are using an external Cd/DVD/Blu-Ray drive, USB attach it to the Windows computer now



3. Insert a blank disc and close the door to the external drive.



4. Because you inserted a blank disc, Windows will pop-up a dialog asking how you would like to use the disc. You can either close this dialog or just ignore it since we are going to use secRMMSafeCopy to create an encrypted disc.

Burn a Disc	×
How do you want to use this disc?	
Disc title: Mar 09 2025	
Like a USB flash drive     Save, edit, and delete files on the disc anytime. The disc will     work on computers running Windows XP or later. (Live File     System)	
<ul> <li>With a CD/DVD player</li> <li>Burn files in groups and individual files can't be edited or removed after burning. The disc will also work on most computers. (Mastered)</li> <li>Which one should I choose?</li> </ul>	
Next Cance	9

5. secRMMSafeCopy will see the blank disc. Note that the CD Drive will show up in both the left and right lists. The list on the left is what Windows sees (similar to Windows explorer) and the list on the right is what secRMM is monitoring/managing.

🔒 secRMM SafeCopy	- 0	×
File Settings Tools Help		
secRMM SafeCo	ору	? Help
Refresh Add Copy	Refresh New folder Delete	
⊡ — Drives	🖃 🖷 🧯 Removable Media	
	CD Drive (F:)	
CD Drive (F:)		
User: W9\user1 Computer: W9 New device added.		:

6. In the right hand list of secRMMSafeCopy, right mouse click on the CD drive and select the 'Encrypt Cd' option

🔋 secRMM SafeCopy	– 🗆 X
File Settings Tools Help	
secRMM SafeC	opy 🤗
Refresh Add Copy	Refresh New folder Delete
	F:
⊡ Drives	🖃 🔴 Removable Media
⊕OS (C:) ⊕D drive (D:)	CD Drive (Delete
CD Drive (F:)	Paste
	Properties
	Encrypt Cd
User: W9\user1 Computer: W9 New device added	. Unmount Cd

- 7. Fill in the following:
  - a. Password

Note that the icon to the right of this field will change color as your password strength changes. Red is weak, Yellow is medium and Green is strong. Also, BitLocker requires that the password be at least 8 characters long.

- Folder where the data files are located Note that there is a button to the right of this field that shows you the folders on your computer.
- c. Finalize Cd (i.e. make it write protected after the disc is burned/created)
- d. The data classification (which is included in the report) Note that the data classification checkboxes change when you click them twice (not once).

secRMM SafeCopy Encr	ypt CD/DVD/Blu-Ray disc		×
Please specify the followi	ng values:		
Password:	0		
		Show	
Please selct folder where	files are located (optional):	••••	
<ul> <li>✓ Finalize Cd</li> <li>Data classification:</li> <li>✓ Unclassified</li> <li>Confidential</li> <li>Secret</li> <li>Top Secret</li> </ul>	?		
<< First	< Previous	Next >	Last >>

Click the Next button once you have specified the values above.

secRMM SafeCopy Encrypt C	D/DVD/Blu-Ray disc		
Please specify the following va	ues:		
Password:	?		
•••••		🧹 🗌 Show	
Please selct folder where files	re located (optional):	•	
D:\_MyCorporation\DOD_Doc	uments\Classified		
Prinaitze Cd   Data classification:    Unclassified   Confidential   Secret   Top Secret			
<< First	< Previous	Next >	Last >>

8. You can now review the information about this encrypted disc creation. If you are satisfied with the information, you can click the 'Next' button or go back to make any changes by clicking the 'Previous' button.

secRMM SafeCopy Encrypt CD/DVD/Blu-Ray disc		×
You are about to create an encrypted disc for the following:		
*** DATA CLASSIFICATION: Secret ***	^	
Date: 2025:03:09 12:46:20 PM		
UserName: W9\user1		
ComputerName: W9		
This disc creation was approved by: NOT REQUIRED		
Drive: F		
Vendor Id: Dell		
Product Id: DVD+/-RW DW316		
Physical Media Type: CD-RW		
File system: Blank		
Imedia status: Biank, Appendable		
Total: 847 602 000 (808 34 MB)		
Used: 1,241,856 (1.18 MB)		
Free: 844,262,992 (805.15 MB)		
Copying folder:		
D:\wyCorporation\DOD_Documents\Classified Size: 10.854 (10.60 KB)		
Files: 3		
The disc will be finalized after copying the folder above.	<u> </u>	
	•	
<_ First Provious	Nexts	Lastas
CCTIISE CTIEVIOUS	IVEXL >	Ldst 22

9. The creation of the encrypted disc will now start. Please be patient, this might take a while to complete. You will also see 'Windows explorer' windows opening and closing. This is normal/expected.

File system: Blank       A         Media status: Blank, Appendable       Space:         Total: 847,602,000 (808.34 MB)       Used: 1,241,856 (1.18 MB)         Used: 1,241,856 (1.18 MB)       Free: 844,262,992 (805.15 MB)         Copying folder:       D:\_MyCorporation\DOD_Documents\Classified         Size: 10,854 (10.60 KB)       Files: 3         The disc will be finalized after copying the folder above.         Calling CreateCd.ps1         Start date/time: 2025:03:09 12:49:53 PM (yyyy:MM:dd hh:mm:ss tt)	
Copying folder: D:\_MyCorporation\DOD_Documents\Classified Size: 10,854 (10.60 KB) Files: 3 The disc will be finalized after copying the folder above. Calling CreateCd.ps1 Start date/time: 2025:03:09 12:49:53 PM (yyyy:MM:dd hh:mm:ss tt)	
Formating Cd	
Creating encrypted Cd	

- 10. Once the encrypted disc is created:
  - a. The Finish button will become enabled
  - b. A print button will become visible so you can print the status/report (optional)
  - c. The newly created encrypted disc will eject from the disc drive

e secRMM SafeCopy Encrypt CD/DVD/Blu-Ray disc	×
<pre>Encrypted disc creation status/report:</pre> Encrypted disc creation status/report: Encrypted disc creation status/report: Calling EncryptVhd for C:\Users\Tony\AppData\Local\Temp\EncryptedDataFromCd_FileBook (Disers\Tony\AppData\Local\Temp\EncryptedDataFromCd_FileBook (Di	Print
	Finish

To use the data files on the encrypted disc, the end-user will need to unlock it using the password specified to create the encrypted disc. Instructions on unlocking an encrypted disc are explained in the section of this document titled "Unlock an encrypted disc".

#### Preapproval (two man policy)

Your security environment might be setup so that when you create an encrypted disc, the process of doing so will need to be approved by another person. If this is the case for your environment, when you perform the steps above, you will also see a window that will require the approval (to create an encrypted disc). You can see that in the screenshot below. Note that the information in this window will most likely reflect information about your company/organization. The screenshot below is only an example.

Preapproval Required		
Company	Please either: email <u>security@mycompany.com</u> or call 702.123.1234 to get approval	^
NOTE: Before you begin operation you perform wh mapping to network share	using secRMM SafeCopy, you need to understand that every ile using secRMM SafeCopy (i.e. copying files, deleting files and s) is being logged.	~
	Cancel OK	

Once the approval process has been performed, you can continue creating the encrypted disc following the steps above. Note that the status/report will show who approved the creation of the encrypted disc as shown in the screenshot below.

💿 secRMM SafeCopy Encrypt CD/DVD/Blu-Ray disc	×
<ul> <li>secRMM SafeCopy Encrypt CD/DVD/Blu-Ray disc</li> <li>You are about to create an encrypted disc for the following:</li> <li>*** DATA CLASSIFICATION: Secret ***</li> <li>Date: 2025:03:10 12:08:52 PM</li> <li>UserName: W9/User1</li> <li>ComouterName: W9</li> <li>This disc creation was approved by: W9\Tony</li> <li>Drive: E:</li> <li>Vendor Id: Dell</li> <li>Product Id: DVD+/-RW DW316</li> <li>Physical Media Type: CD-RW</li> <li>File system: Blank</li> <li>Media status: Blank, Appendable</li> <li>Space:</li> <li>Total: 847,602,000 (808.34 MB)</li> <li>Used: 1.241.856 (1.18 MB)</li> <li>Free: 844,262,992 (805.15 MB)</li> <li>Copying folder:</li> <li>D:M/Copporation\DDD_Documents</li> <li>Size: 10.854 (10.60 KB)</li> <li>Files: 4</li> <li>The disc will be finalized after copying the folder above.</li> </ul>	×
<< First < Previous Next > Last >>	

If the approver rejects your request to create an encrypted disc, you will see the following 2 windows and the creation of the encrypted disc will be unable to continue.

Approver: W9\Tony Approval: Rejected	
Cancel OK	.::
Details Required × Current page is not valid. Please correct the information Preapproval did not complete successfully	

You must click the close button (as shown in the screenshot below) until you can get proper approval to create an encrypted disc.



## Unlock an encrypted disc

Please follow the steps and screenshots in this section to unlock an encrypted disc. There are 3 ways to unlock an encrypted disc created by secRMMSafeCopy:

1. Use secRMMSafeCopy

secRMM SafeCopy		- 0	×
File Settings Tools Help			
Exit	secRMM SafeCopy		? Help
Refresh Add Copy	Refresh New folder Delete		
Drives Drives Drive (D:) CD Drive (F:)	F: Removable Media Right click CD Drive (E-) Delete Paste Properties Unlock Cd Unmount Cd	the CD	
User: W9\user1 Computer: W9			:

- 2. Use the UnlockEncryptedCd.exe program that resides on the encrypted disc under the folder named EncryptedDataUtilities on a computer that has secRMM installed.
- 3. Use the UnlockEncryptedCd.exe program that resides on the encrypted disc under the folder named EncryptedDataUtilities on a computer that does not have secRMM installed.



All 3 options above will display the UnlockEncryptedCd program as shown below. Provide the password used to create the encrypted disc. Please note there is no way to recover the password if you forget it<sup>2</sup>.

<sup>&</sup>lt;sup>2</sup> Please see the section below titled 'Overriding Enable-BitLocker' that describes how to create a recovery key in case of a forgotten password.

secRMM SafeCopy - Unlock encrypted Cd/Dvd/Blu-Ray	
Please enter the password	Settings
OK Cancel	

Once you specify the password and click the OK button, the encrypted data will become available on the computer. Please be patient, it can take some time for the data to be copied from the encrypted disc to a temporary directory where you can work with the data files.

secRMM SafeCopy - Unlock encrypted Cd/Dvd/Blu-Ray	
Please enter the password	Settings
OK Cancel Please wait, unlocking encrypted Cd	

You will most likely get a pop-up message box from Windows explorer telling you 'Access is denied'. This is a timing issue/bug between BitLocker and Windows Explorer. You can simply click the OK button to dismiss it. We are working on a way to fix this annoying issue/bug.

Locatio	on is not available	×
8	Z:\ is not accessible. Access is denied.	
		ОК

Once the encrypted data becomes available, you will get a pop-up message box telling you which drive letter you can use to access the encrypted data. This is shown in the screenshot below. In this example, the encrypted data is now available on the Z: drive.

secRMM SafeCopy - Unlock encrypted Cd The encrypted data from Cd F: is You can acces it on the Z: drive in or from the secRMM SafeCopy pu Please use the 'Unmount Cd' fro when you are finished using the	/Dvd/Blu-Ray now available. N Windows explorer rogram. m secRMM SafeCopy encrypted Cd data.	×
🚔   🛃 🤿   Local Disk (Z:)	Manage	×
Pin to Quick Copy Paste	Drive Tools	Properties
← → < ↑ 🚔 > This PC > Loca	al Disk (Z:)	v ē Search Lo ♪
<ul> <li>This PC &gt; Local</li> <li>Quick access</li> <li>OneDrive - Personal</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Wideos</li> <li>S OS (C:)</li> <li>D drive (D:)</li> <li>OVD RW Drive (F:) 2025.03.09_125</li> <li>EncryptedDataUtilities</li> <li>Local Disk (Z:)</li> </ul>	Name ClassifiedD	ocument1.txt ocument2.txt ourcesData_Q1_2012.zip
3 items		

. . . . .

, -----

Once you are finished using the encrypted data, you should 'Unmount' the encrypted Cd which is explained in the next section of this document. Failure to unmount the encrypted Cd will leave the encrypted temporary drive (the Z: drive in our example above) mapped to Windows. Although there is nothing wrong with that, it may be annoying to the end-users. The drive will be temporary and a reboot of Windows will remove the temporary drive (if you do not perform the unmount as recommended). Please read the details in the next section for more information.

## **Unmount an encrypted disc**

Please follow the steps and screenshots in this section to unmount an encrypted disc. There are 3 ways to unmount an encrypted disc created by secRMMSafeCopy:

1. Use secRMMSafeCopy



- 2. Use the UnmountCd.exe program that resides on the encrypted disc under the folder named EncryptedDataUtilities on a computer that has secRMM installed.
- 3. Use the UnmountCd.exe program that resides on the encrypted disc under the folder named EncryptedDataUtilities on a computer that does not have secRMM installed.

#### secRMM Administrator Guide

📙   🛃 🚍 🖛 l EncryptedDataUtilities	
File Home Share View	
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\square$ $\Rightarrow$ This PC $\Rightarrow$ DVD RW	/ Drive (F:) 2025.03.09_1251 > EncryptedDataUtilities
<ul> <li>&gt; A Quick access</li> <li>&gt; OneDrive</li> <li>&gt; This DC</li> </ul>	Name V Files Currently on the Disc (8) CommonCd.ps1 FinalizeDisc cmd
<ul> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>S OS (C:)</li> <li>D drive (D:)</li> <li>D DVD RW Drive (Ei) 2025 02 09, 1251</li> </ul>	<ul> <li>FinalizeDiscexe</li> <li>GetCdInfo.ps1</li> <li>UnlockEncryptedCd.exe</li> <li>UnlockEncryptedCd.ps1</li> <li>UnmountCd.exe</li> <li>UnmountCd.ps1</li> </ul>
<ul> <li>EncryptedDataUtilities</li> <li>Local Disk (Z:)</li> <li>OVD RW Drive (F:) 2025.03.09_1251</li> <li>Metwork</li> </ul>	

All 3 options above will display the UnmountCd program as shown below.

secRMM SafeCopy - Unmount Cd/Dvd	/Blu-Ray
Save encrypted data back to Cd Finalize Cd	Settings
OK Cancel	

For most use cases, you will ignore the 2 checkboxes on this screen and simply click the OK button. The unmount will remove the temporary drive where the encrypted data was and eject the Cd drive.

The 2 checkboxes can be used if you did not finalize (i.e. not make it write protected) when you created the encrypted disc. If you did not finalize the encrypted disc, you can add and remove files as if it were a usb thumb drive device.

## Using an encrypted disc where secRMM is not installed

#### Using the secRMM provided programs on the disc

Both the UnlockEncryptedCd and UnmountCd programs can be accessed directly on the encrypted disc under the folder named EncryptedDataUtilities. When you run these programs on a computer where secRMM is not installed, you will need to run them as an Administrator account on the computer. To do this, right click the program (i.e. UnlockEncryptedCd.exe or UnmountCd.exe) and select 'Run as administrator'. Note that if your Account is an Administrator account, you still need to right click the program (i.e. UnlockEncryptedCd.exe or UnmountCd.exe) and select 'Run as administrator'. The reason for this is to make sure that the UAC elevated process token is used. The process token needs to be elevated because mounting a 'Virtual Hard Drive' (VHD) requires Administrator permissions. When secRMM is installed on the computer, then secRMM takes care of this for the user, however, when secRMM is not installed, you have to elevate the program as discussed in this section (i.e. 'Run as administrator').

🔜   🗹 🔜 🖵	Manage	EncryptedDat	aUtilities	-		×
File Home Share View	Application Tools					~ ?
Pin to Quick Copy Paste Clipboard	to • X Delete • to • A Pename Organize	New folder New	Properties	Select	t all t none t selection lect	
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\bullet$ DVD RW Drive (F:)	2025.03.09_1251 >	EncryptedDataU	tilities	~ ∂	Search En.	. ,o
<ul> <li>Quick access</li> <li>OneDrive - Personal</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>OS (C:)</li> <li>D drive (D:)</li> <li>DVD RW Drive (F:) 2025.03.09_1251</li> <li>EncryptedDataUtilities</li> <li>Network</li> </ul>	Name V Files Current CommonC FinalizeDisc. FinalizeDisc. GetCdInfo.p OunlockEncry UnlockEncry UnmountCd UnmountCd	ly on the Disc d.ps1 cmd .exe s1 ptedCd.exe ptedCd.exe l.ps1	(8) (8) (9) (9) (9) (9) (9) (9) (9) (9) (9) (9	Date modifie 3/8/2025 12: 5/25/2018 5: 3/9/2025 11: 3/9/2025 12: 3/9/2025 11: ator mpatibility soft Defend	ed 45 PM 44 PM 12 AM 30 PM 07 AM	Type Win App Win Anp > >
i Network			Create shortcut Properties			



Failure to use 'Run as administrator' will result in an error message as shown in the screenshot below.

#### **Using Windows Explorer**

You can use Windows Explorer to mount and unmount the "EncryptedData.VHD" file that resides on the disc. You will need to be a local or domain administrator to perform these operations.

#### Unlock an encrypted disc

Copy the file named "EncryptedData.VHD" (in the root folder) from the disc to any NTFS drive your computer can access.

## secRMM Encrypted CD/DVD/Blu-ray User Guide



Right mouse click on the "EncryptedData.VHD" file (that you just copied to the NFTS drive). Select "Mount".

📕   🗹 📕 =	Manage	MyData	_	
File Home Share View	Disc Image Tools			~ ?
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\blacksquare$ $\rightarrow$ This PC $\rightarrow$ W	indows (C:) → temp	p → MyData	ン O Search M	/lyData 🔎
b Music	^ Nat	me Right click	Date modified	Туре
Pictures	-	EncryptedData.VHD	2/14/2025 11:44 AM	Disk Image F
📕 Videos			Mount	
🐛 Windows (C:)			Share with Skype	
DVD RW Drive (D:) 2025.03.14_	1118		Scan with Microsoft Defender	
< d (\\w9) (X:)	~ <		🖻 Share	
1 item 1 item selected 64.0 MB			Open with	
-			Restore previous versions	
			Send to	>
			Cut	
			Сору	
			Create shortcut	
			Delete	
			Rename	
			Properties	

When you click the "Mount", Windows will map a new drive (the Z: drive in the screenshots/example below). The Z: drive needs a password to be able to access it. In the lower right-hand corner of the screen, a pop-up windows will prompt you to "Unlock drive Z:" (it will indicate that "This drive is

BitLocker-protected"). You can click this pop-up window and specify the password. Unfortunately, this pop-up windows will go away in 5 seconds or so. If it does go away, you then need to right-click on the mapped drive (again Z: in our example) and select the "Unlock Drive..." (or you can just click the drive).



## secRMM Encrypted CD/DVD/Blu-ray User Guide



Either way you select to unlock the drive, you will get a window that will prompt you for the password.

BitLocker (Z:)		
Enter password to unlock this drive.		
	<b>^</b>	
	Unlock	

Now specify the password to be able to access the data files.



#### Misleading Windows Explorer pop-up error message

If you are trying to mount the VHD and you are getting an error like the screenshot below, then the "EncryptedData.VHD" has already been mapped to a drive and at this stage, it needs to be unlocked with a password.



If you see this error, look for a drive with the BitLocker icon as in the screenshot below.



Click or right click and select "Unlock Drive...".

#### **Unmount an encrypted disc**

To unmount the mapped drive (i.e. the BitLocker encrypted VHD from above), right mouse click the drive and select "Eject".

	Expand
	Open AutoPlay
	Scan with Microsoft Defender
$\begin{array}{c c} \hline File & Home & Sha \\ \hline $	Change BitLocker password Manage BitLocker
<ul> <li>S This PC</li> <li>S D Objects</li> </ul>	Pin to Quick access Give access to > Restore previous versions
<ul> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> </ul>	Include in library
> 🎝 Music	Eject
> E Pictures	Сору
> 💺 Windows (C:)	Rename
> 💿 DVD RW Drive ([	New >
> 🛹 d (\\w9) (X:) > 🤳 Local Disk (Z:)	Properties
<ul> <li>DVD RW Drive (D:) 202</li> <li>EncryptedDataUtilities</li> </ul>	5.03.14_1118 s

## Administrator/Advanced section

#### **PowerShell**

All of the information above helps end-users create and use the secRMM encrypted discs. All of the operations performed for the end-users are done using PowerShell scripts even though they cannot tell from the secRMMSafeCopy GUI programs. The PowerShell scripts are all located under C:\Program Files\secRMM\UserUtils\CdDvdBluray folder. If your environment requires unique items for encrypted discs, we are hopeful they can be accomplished by modifying the PowerShell scripts. If you find yourself needing to modify the PowerShell scripts, we are happy to assist in any way we can. Please just email <u>support@squadratechnologies.com</u> and we can make a plan together.

#### **Overriding Enable-BitLocker**

Some environments may want to extend the encryption performed by BitLocker. Perhaps to save the BitLocker recovery key(s) to a network share, just in case the password is forgotten. To accomplish this, you would create a file in C:\Program Files\secRMM\UserUtils\CdDvdBluray named **Enable-BitLocker-Override.ps1**. Within Enable-BitLocker-Override.ps1, you can call the PowerShell Enable-BitLocker command using parameters and/or code that better suits your security environment. Below is a sample Enable-BitLocker-Override.ps1. This example saves the BitLocker recovery key to a network share. Once again, please reach out to 'squadra technologies support' and we are happy to help with this customization.

```
Module: Enable-BitLocker-Override.ps1
#
#
#
  Purpose: Override the default Enable-BitLocker called by EncryptCd.ps1.
                  Put this script/file in directory:
#
                  "C:\Program Files\secRMM\UserUtils\CdDvdBluray"
#
#
#
  Copyright (c) 2024 Squadra Technologies
#
#
  Defined PowerShell variables available to use:
  $stringVhdDriveLetter_in =
#
            The drive letter of the VHD being encrypted (ex: Z:).
#
  $g_EncryptionStrength =
#
            "Aes256"
#
#
  $stringPassword_in =
           The password specified by the user.
#
#
  $stringCdDriveLetter_in =
#
            The CD drive letter where the VHD will reside (ex: E:)
```

```
$1_stringNetworkShare = "\\Server\Share"; # change this line for your environment
$1_secureStringPassword = ConvertTo-SecureString -String $stringPassword_in -AsPlainText -Force;
Enable-BitLocker
-MountPoint $stringVhdDriveLetter_in `
-EncryptionMethod $g_EncryptionStrength
-UsedSpaceOnly `
-Password $1_secureStringPassword `
-PasswordProtector
-ErrorVariable ErrorEnableBitLocker
-ErrorAction SilentlyContinue | Out-Null;
if (($ErrorEnableBitLocker -eq $null) -or `
       ($ErrorEnableBitLocker.Count -eq 0)) {
       while ( (Get-BitLockerVolume -MountPoint $stringVhdDriveLetter_in).VolumeStatus -ne "FullyEncrypted" )
       {
               Start-Sleep -Seconds 5;
       }
}
Add-BitLockerKeyProtector `
   -MountPoint $stringVhdDriveLetter_in `
   -RecoveryPasswordProtector| Out-Null;;
$1_stringRecoveryKey =
(Get-BitLockerVolume -MountPoint $stringVhdDriveLetter_in).KeyProtector
| Where-Object {$_.KeyProtectorType -eq 'RecoveryPassword'};
$1_stringRecoveryKeyFileName =
("{0}_{1}_{2}_EncryptedCD_BitLocker.txt" -f `
       $env:COMPUTERNAME,
       $stringVhdDriveLetter_in.Substring(0, 1), `
       $stringCdDriveLetter_in.Substring(0, 1));
if ((Test-Path -Path $1_stringNetworkShare) -eq $true) {
       $1_stringRecoveryKeyCompleteFileName =
               Join-Path -Path $1_stringNetworkShare -ChildPath $1_stringRecoveryKeyFileName;
}
else {
       # NOTE: This may not be a valid solution for your environment!
       #
               Since the network folder is not found, put it in the temp directory
       $1_stringRecoveryKeyCompleteFileName =
               Join-Path -Path $env:TEMP -ChildPath $1_stringRecoveryKeyFileName;
}
```

```
$1_stringRecoveryKey.RecoveryPassword | `
```

Out-File -FilePath \$1\_stringRecoveryKeyCompleteFileName;

# EncryptCd.ps1 function EncryptVhd uses these 3 variables for status

\$1\_intReturnCode = 0;

\$1\_stringReturnData = \$null;

\$1\_stringErrorMessage = \$null;xxxx

#### Using the PowerShell scripts without a GUI

You may need to call the functionality provided by secRMM's disc encryption without using secRMMSafeCopy or perhaps you want to incorporate it into your own User Interface. All of the scripts reside in the secRMM subdirectory UserUtils\CdDvdBluray. You will need to run these with an Administrator account and with UAC='Run As Administrator'.

Here are the main scripts:

1. CreateCd.ps1

.\CreateCd.ps1 -stringCdDriveLetter\_in e -stringPassword\_in MyPassword!1 stringFolderWithFiles\_in D:\MyFolder -intFinalizeCd\_in 1

2. UnlockEncryptedCd.ps1

.\UnlockEncryptedCd.ps1 -stringVhdCompleteFilePath\_in E:\EncryptedData.VHD stringPassword\_in MyPassword!1 -stringDriveLetterForVhd\_in Z:

3. UnmountCd.ps1

.\UnmountCd.ps1 -stringCdDriveLetter\_in e -stringMountOrAccessPoint\_in z

4. GetCdInfo.ps1

\GetCdInfo.ps1 -stringCdDriveLetter\_in e

Note that each one of these scripts relies on the script \_CommonCd.ps1 to be in the same directory. If you are looking to use the scripts please reach out to `squadra technologies support' and we are happy to help.

#### Debugging

You should encourage your end-users to turn on debugging mode when working with the encrypted discs. In an event where there is an issue, you (and/or Squadra Technologies support) can review the debug logs to identify any issues.

To turn on debugging in the secRMMSafeCopy program, use the main menu bar: Settings->Debug.

🖼 secRMM SafeCopy	– 🗆 X
File Settings Tools Help	
Copying Exit Debug secRMM SafeCo	py 🤗
Refresh Add Copy	Refresh New folder Delete
⊡ <mark></mark> Drives	Removable Media
User: W9\Tony Computer: W9	.::

When debugging is turned on, it will look like:

🔋 secRMM SafeCopy		_	×
File Settings Tools Help			
Copying Exit Copying secRMM SafeCo	ру		? Help
Refresh Add Copy	Refresh New folder	Delete	
	Aremovable Media		
User: W9\Tony Computer: W9			

Please note the checkbox indicating that the debugger is turned on is not aligned correctly. This is a Microsoft .Net issue. Once they resolve this issue, we will incorporate it into the secRMMSafeCopy program.

If your end-users are invoking the UnlockEncryptedCd and UnmountCd programs directly from the secRMMSafeCopy program, the debug flag will be passed down to them when they are called. If they call the UnlockEncryptedCd and UnmountCd programs directly (i.e. not from secRMMSafeCopy), they can click the "Settings" button to turn on debugging. You can see that in the screenshots below.

secRMM SafeCopy - Unlock encrypted Cd/Dvd/Blu-Ray	💿 secRMM SafeCopy - Unlock encrypted Cd/Dvd/Blu-Ray - Settings 🛛 - 🔲 🗙
Please enter the password Settings	Please select an existing Vhd file created by SafeCopy and how to map it to be online.
OK Cancel	Vhd:
	Map Vhd to:
	Folder
	☑ Drive Z ∽
	Debug
	OK Cancel

secRMM SafeCopy - Unmount Cd/Dvd/Blu-Ray	💿 secRMM SafeCopy - Unmount Cd/Dvd/Blu-Ray - Settings 🛛 — 🛛 🗙
Save encrypted data back to Cd Sattings	Please select an existing Cd drive letter and MountOrAccessPoint created by SafeCopy.
Finalize Cd	Cd drive letter :
OK Cancel	MountOrAccessPoint:
	✓ Debug
	OK Cancel

If you are calling the PowerShell scripts directly, use parameters:

- 1. -intDebug\_in
- A value of 1 turns debugging on
  2. -stringOutputErrorDebugFilesFolder\_in Specify an existing directory where you want the debug file(s) (file extension will be .log) to go

PS C:\Program Files\secRMM\UserUtils\CdDvdBluray> .\GetCdInfo.ps1 -stringCdDriveLetter\_in E: -intDebug\_in 1 -stringOutputErrorDebugFilesFolder\_in C:\temp|

#### **Debug file locations**

If secRMM is installed on the computer, the debug files will be located in:

"C:\Program Files\secRMM\UserUtils\CdDvdBluray\OutputErrorDebugFiles".

The debug files will all end with the file extension ".log".

## secRMM Administrator Guide

📕   📝 📜 🔻   OutputErrorDebugFiles				- 0	×
File Home Share View					~ ?
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ ] > This PC > Windows (C:)	Program Files > secRMM > UserUtils > CdDvdBluray >	OutputErrorDebugFiles	× گ	Search OutputError	,P
	Name	Date modified	Туре	Size	
> 📌 Quick access	CreateCd.ps1.log	3/12/2025 11:28 AM	LOG File	4 KB	
> 🥌 OneDrive	CreateCd_2025.03.12_1103.rpt	3/12/2025 11:42 AM	RPT File	4 KB	
OneDrive - Personal	EncryptCd.ps1.log	3/12/2025 11:28 AM	LOG File	12 KB	
	EncryptCd.ps1.out	3/12/2025 11:28 AM	OUT File	1 KB	
🗸 🍃 This PC	EncryptCd.ps1.RoboCopy_2025-03-12_11-26-40.log	3/12/2025 11:26 AM	LOG File	2 KB	
> 🧊 3D Objects	FormatCd.ps1.err	3/12/2025 11:26 AM	ERR File	1 KB	
> 🔜 Desktop	FormatCd.ps1.log	3/12/2025 11:26 AM	LOG File	5 KB	
> 🗄 Documents	🚺 GetCdInfo.ps1.log	3/12/2025 11:26 AM	LOG File	6 KB	
> 🕂 Downloads	GetCdInfo.ps1.out	3/12/2025 11:26 AM	OUT File	2 KB	
> 🎝 Music	扪 UnlockEncryptedCd.ps1.log	3/12/2025 11:37 AM	LOG File	4 KB	
> 📰 Pictures	UnlockEncryptedCd.ps1.out	3/12/2025 11:37 AM	OUT File	1 KB	
> Videos	UnmountCd.ps1.log	3/12/2025 11:38 AM	LOG File	3 KB	
> 🐛 Windows (C:)	UnmountCd.ps1.out	3/12/2025 11:38 AM	OUT File	1 KB	
> OVD RW Drive (D:) 2025.03.12 1127					
> 👽 d (\\w9) (X:)					
<ul> <li>DVD RW Drive (D:) 2025.03.12_1127</li> </ul>					
EncryptedDataUtilities					
> 学 Network					
13 items					:==

If secRMM is not installed on the computer, the debug files will be located in the users temporary (TEMP environment variable) directory as shown in the screenshot below.



## secRMM Encrypted CD/DVD/Blu-ray User Guide

# Troubleshooting

When you insert a new/blank disc and right mouse click on the CD in secRMMSafeCopy, sometimes, you will not see the "Encrypt Cd" menuitem. The issue seems to resolve itself if you open the Cd door and then close it again. In addition, you can check the state of the disc by turning on trace data (see first screenshot below) and then right mouse clicking the Cd icon again. The second screenshot below shows the state of a disc where secRMMSafeCopy will show you the "Encrypt Cd" menuitem.

# secRMM Administrator Guide

🔋 secRMM SafeCopy			_	$\times$
File Settings Tools Help				
Copying 🕨	Show details			2
Exit Debug	Practice mode			Help
🛛 🕞 🛼 📥 💆	Show trace	- 🦂 🗙	-	
Refresh Add Copy	CD info - use SYSTEM	New folder Dele	te	
	D:			
Drives     Windows (C:)     DVD RW Drive (D:)     d (\\w9) (X:)		emovable Media DVD RW Drive (D:)		
User: CONTOSO\Administrator	omputer: SECRMMDEMO2			.::

### secRMM Encrypted CD/DVD/Blu-ray User Guide

🕞 secRMM SafeCopy	- 🗆 X
File Settings Tools Help	
secRMM SafeCo	py 🤗 💦
Refresh Add Copy	Refresh New folder Delete
⊡⊡ Drives 	E
 ⊡	CD trace data × IsMediaLoaded: True IsMediaFormated: False IsMediaSWriteProtected: False IsMediaMounted: False IsMediaSEncryptedDataUnlocked: False FreeSpace: 846360144
User: CONTOSO\Administrator Computer: SECRMMDEM	О2

## **Known issues**

1. Sometimes secRMMSafeCopy misses events from the Windows operating system when disk drives get added and/or removed. You can use the refresh buttons if you see or do not see a drive. We are working on a way to make this more reliable.

📑 sec	RMM Safe	Сору								_		×
File	Settings	Tools	Help									
Exit				sec	RMM Safe	eCopy	/					? Help
Refree	sh Add	Сору					Carlor Refresh	Den folde	r Delete			
	Drives Drives Winde ■ DVD ■ DVD ■ d (\\w	ows (C:) RW Drive v9) (X:)	(D:)		<b>`</b>			emovable Med	dia krive (D:)		<b>`</b>	
User: C	ONTOSO\A	dministra	ator Co	mput	er: SECRMM	DEMO2	New de	evice added.				.::

2. When burning a disc, the green progress bar is not able to stay in sync exactly with the burn process. It will look like it is almost complete when there is really more work to be done.



3. The secRMMSafeCopy program shows the BitLocker encrypted container with the wrong icon. We are working on a solution to this issue.

🖼 secRMM SafeCopy	<b>\</b>	– 🗆 X
File Settings Tools Help		
Exit	secRMM S&feCopy	? Help
Refresh Add Copy	Refresh N	ew folder Delete
Drives Drives		vable Media         //D RW Drive (E:)         EncryptedData.VHD
User: W9\Tony Computer: W9 Ne	w device added.	

4. When the BitLocker enabled VHD mounts, Windows Explorer sometimes shows a message saying the drive is not accessible.

This is a timing issue/bug between BitLocker and Windows Explorer. You can simply click the OK button to dismiss it. We are working on a way to fix this annoying issue/bug.

Location is not available					
$\otimes$	Z:\ is not accessible. Access is denied.				
	ОК				

5. When the BitLocker enabled VHD mounts, the Windows System event log gets many error messages where the 'Source' column is 'FilterManager' and the 'Event ID' column is 3. This appears to be related to the 'Windows Search Service'. While annoying, it does not cause any issues. We are working on a way to fix this annoying issue/bug.

🛃 Event Viewer								— C	×
File Action View Help									
🗢 🔿 🙍 🖬									
la Event Viewer (Local)	<b>System</b> Number of	of events: 2,533 (!) Nev	w events available				Act	ions	
Custom Views	Level Date a	nd Time	Source	Event ID	Task Category	^	Sys	tem	▲ ^
Windows Logs     Application	Error 3/12/2	025 11:26:44 AM	FilterManager	3	None		1	Open Saved Log	
Security	U Error 3/12/2	025 11:26:44 AM	FilterManager	3	None		-	Create Custom View	
Setup	Error 3/12/2	025 11:26:44 AM	FilterManager	3	None		L.	Import Custom View	
System	Error 3/12/2	025 11:26:44 AM	FilterManager	3	None		- I	import custom view	
Forwarded Events	Error 3/12/2	025 11:26:44 AM	FilterManager	3	None		L	Clear Log	
Applications and Services Logs	Error 3/12/2	025 11:26:44 AM	FilterManager	3	None	~	7	Filter Current Log	
Event 3, FilterManager								Properties	
				000	Find				
	General Details							Save All Events As	
	Filter Manager 6	destas saturals to contr	ND is a literated	i - LA / - La	7. This column souill	^	1.04	Save All Events As	
	unavailable for f	lifed to attach to voli Itering until a reboo	t. The final status wa	iskvolume5 as 0xC03A00	). This volume will )1C.	be	- I	Attach a lask to this Log	
		,				-11		View	•
	Log Name:	Sustem					Q	Refresh	
	Source	FilterManagor	Logged	· 3/1	12/2025 11·26·44 AM		?	Help	•
	Event ID:	2	Task Ca	tegona Na	12/2023 11:20:44 Alv		-		
	Level	Error	Kenned	de	Jie		Eve	ent 3, FilterManager	 <b>^</b>
	Level.	EITOT	Compu	us.		TOSC		Event Properties	
	Oser:	SYSTEM	Compt	iter: see	CRIVINIDemo2.CON	IOSC	1	Attach Task To This Event	
	Opcode:		. Links			~	84	Сору	•
	< Nore information	e eveni i od Online	- Help			>		Save Selected Events	
							1.001	Save Selected Events	~

6. When you look at the file WRITE events for the encrypted drive in secRMM event log, you will see several files being copied that represent the structure of the BitLocker encryption. They go into the "System Volume Information" directory (this is a hidden directory) and the files start with "FVE2." (see screenshot below). This can be annoying when you are running report and/or analyzing the files that are being copied. Although annoying, we are reluctant to modify the lower levels of secRMM from processing these files since that is the main job of secRMM. Please let us know your thoughts on this issue.

### secRMM Encrypted CD/DVD/Blu-ray User Guide

w	102	Previous Next						
	Name	Value						
E	Event	WRITE COMPLETED						
Time Computer User		03/14/2025 01:05:39 PM						
		secRMMDemo2.CONTOSO.com						
		NT AUTHORITY\SYSTEM						
ι	Jser SID	S-1-5-18						
۵	Drive	Z:						
١	/olume	\Device\HarddiskVolume15						
	Local Fixed Disk Fixed hard disk media Win32_LogicalDisk							
5	Serial Number	EEABBB4D						
Ν	Model	Microsoft Virtual Disk						
l	nternal Id	SCSI\DISK&VEN_MSFT&PROD_VIRTUAL_DISK\2&1F4ADFFE&0&000001						
1	Farget File	Z:\System Volume Information\FVE2.{09cf57b8-9e6c-43d4-ae1f-0408882a397d}.1						
5	Source File	Z:\System Volume Information\FVE2.{09cf57b8-9e6c-43d4-ae1f-0408882a397d}.1						
F	<sup>o</sup> rogram Name	SYSTEM						
F	Program PID	4						

7. The secRMMSafeCopy encryption audit records show the SYSTEM account as the user performing the encryption. We are working on a solution to this issue.

secRMM Number of ev	vents: 188					
Level	Date and Time	Source	Event ID	Task Category	^	
<ol> <li>Information</li> </ol>	3/16/2025 8:11:07 AM	secRMM	402	2 AUDIT		
<ol> <li>Information</li> </ol>	3/16/2025 8:11:07 AM	secRMM	402	AUDIT		
<ol> <li>Information</li> </ol>	3/16/2025 8:11:06 AM	secRMM	814	SAFECOPY		
<u>A</u> w	D/16/0005 0.11.00 AMA	DLALA	<u>=00</u>			
Event 402, secRMM					×	
General       Details         Removable Media Security Audit:       Drive: Z;, Volume: \Device\HarddiskVolume17, Desc: Local Fixed Disk ENCRYPTED Fixed hard disk media Win32_LogicalDisk, SerialNumber:         2ADC1044, Model: Microsoft Virtual Disk, InternalID: SCSI\DISK&VEN_MSFT&PROD_VIRTUAL_DISK\2&1F4ADFFE&0&00001         Status: WRITE COMPLETED         Target File: Z:\ClassifiedDocument1.txt         Sources File(c): Du}_McComporation\DOD_Documents\Classified\ClassifiedDocument1.txt, Size: 894, LastWriteTime: 07/13/2012 16:51:56         User: NT AUTHORITY\SYSTEM, SID: S-1-5-18         Program: C:\windows\systemsz\kdocdopy.exe" D:\_MyCorporation\DOD_Documents\Z:\/E/XJ/R:3 /W:5 "/log:C:\Program Files\secRMM         \UserUtils\CdDvdBluray\OutputErrorDebugFiles\EncryptCd.ps1.RoboCopy_2025-03-16_08-11-06.log", PID: 17648						

- 8. Our testing of a Blu-ray drive was not successful. We will work on this issue and post the fix when it becomes available.
- 9. During development and testing, we noticed that many of the discs were defective. The Windows operating system logs an error about the disc having bad blocks (see the screenshot below). If

unlocking the disc seems to hang, check the System event log for the error about the disc having a bad block. If you see this error, you will need to use another disc. We will work on making this condition more visible in the user interfaces. While annoying, we suggest you look in the system event log after you create an encrypted disc to see if the disc has any bad blocks before you give the disc to one of your customers.

🚼 Event Viewer								- 🗆	×	
File Action View Help										
🔶 🧼 🖄 📰 🚺 🖬										
🛃 Event Viewer (Local)	System Number of events: 7,555 () New events available Actions							Actions		
> 📑 Custom Views	Level	Date and Time		Source	Event ID	Task Category	^	System	<b>^</b>	
Application	Error	3/24/2025 11:40:	14 AM	cdrom	7	None	~	open Saved Log		
Security							>	Y Create Custom View		
Setup	Event 7, cdrom						×	Import Custom View		
Forwarded Events	General Details							Clear Log		
> 🖰 Applications and Services Logo	Details							Filter Current Log		
5ubscriptions	The device, \Devic	e\CdRom0, has a bad block.						Properties		
								👭 Find		
								Save All Events As		
								Attach a Task To this Log		
								View	•	
								Refresh		
	'							? Help	•	
	Log Name:	System	Lannah	2/24/2025 11:40-14 654				Event 7, cdrom	<b>^</b>	
	Event ID:	7	Task Category:	None				Event Properties		
	Level:	Error	Keywords:	Classic				Attach Task To This Event		
	User:	N/A	Computer:	W9				Сору	•	
	OpCode:	Info						Save Selected Events		
	More Information:	Event Log Online Help						Q Refresh		
								Help	→	
	h								*	

10.

#### **Contacting Squadra Technologies Support**

Squadra Technologies Support is available to customers who have purchased a commercial version of secRMM and have a valid maintenance contract or who are in a trial mode of the product.

When you contact Support please include the following information:

- 1. The version of secRMM you have installed.
- 2. The Windows versions you have installed: XP, 2003 Server, 2008 Server R2, Vista, Windows 7, Windows 8, Windows 10, Windows 11, etc.
- 3. Whether the Windows Operating System is 32bit or 64bit.
- 4. The specific issue you are contacting support for.

## About Squadra Technologies, LLC.

Squadra Technologies delivers innovative products that help organizations get more data protection within the computer infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Squadra Technologies is helping customers worldwide.

Contacting Squadra Technologies, LLC.

Phone	562.221.3079 (United States and Canada)
Email	info@squadratechnologies.com
Mail	Squadra Technologies, LLC. World Headquarters 4201 State Route W Cleveland, Missouri 64734 USA
Web site	https://www.squadratechnologies.com/