



Security Removable Media Manager

**Encrypted
Cd/Dvd/Blu-ray
User Guide**



Version 9.11.35.0
(March 2025)

Protect your valuable data

secRMM Encrypted CD/DVD/Blu-ray User Guide

© 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.

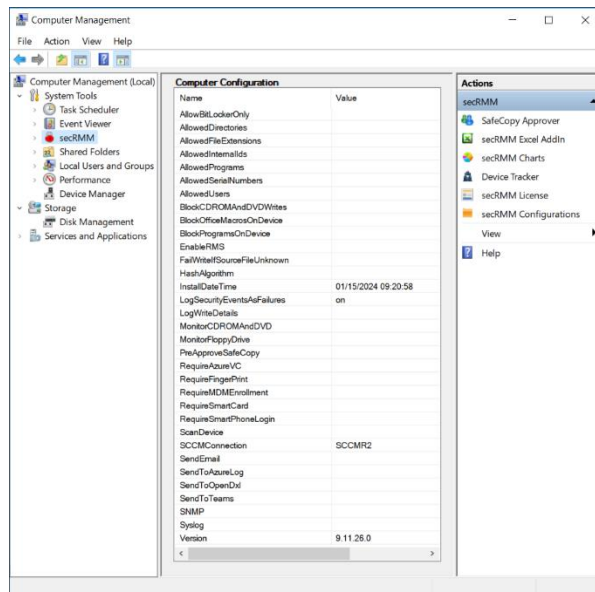
Squadra Technologies Administrator Guide
Created - March 2011

Contents

SECRMM INTRODUCTION	4
SECRMM 'ENCRYPTED DISC' INTRODUCTION	4
ENCRYPTION INFORMATION	5
PREREQUISITES	6
CREATE AN ENCRYPTED DISC	6
<i>Preapproval (two man policy)</i>	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
USING WINDOWS EXPLORER	27
<i>Unlock an encrypted disc</i>	27
Misleading Windows Explorer pop-up error message	31
<i>Unmount an encrypted disc</i>	32
ADMINISTRATOR/ADVANCED SECTION	33
POWERSHELL.....	33
<i>Overriding Enable-BitLocker</i>	33
<i>Using the PowerShell scripts without a GUI</i>	35
DEBUGGING	35
<i>Debug file locations</i>	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 control (or authorize) who can write to the removable media devices.

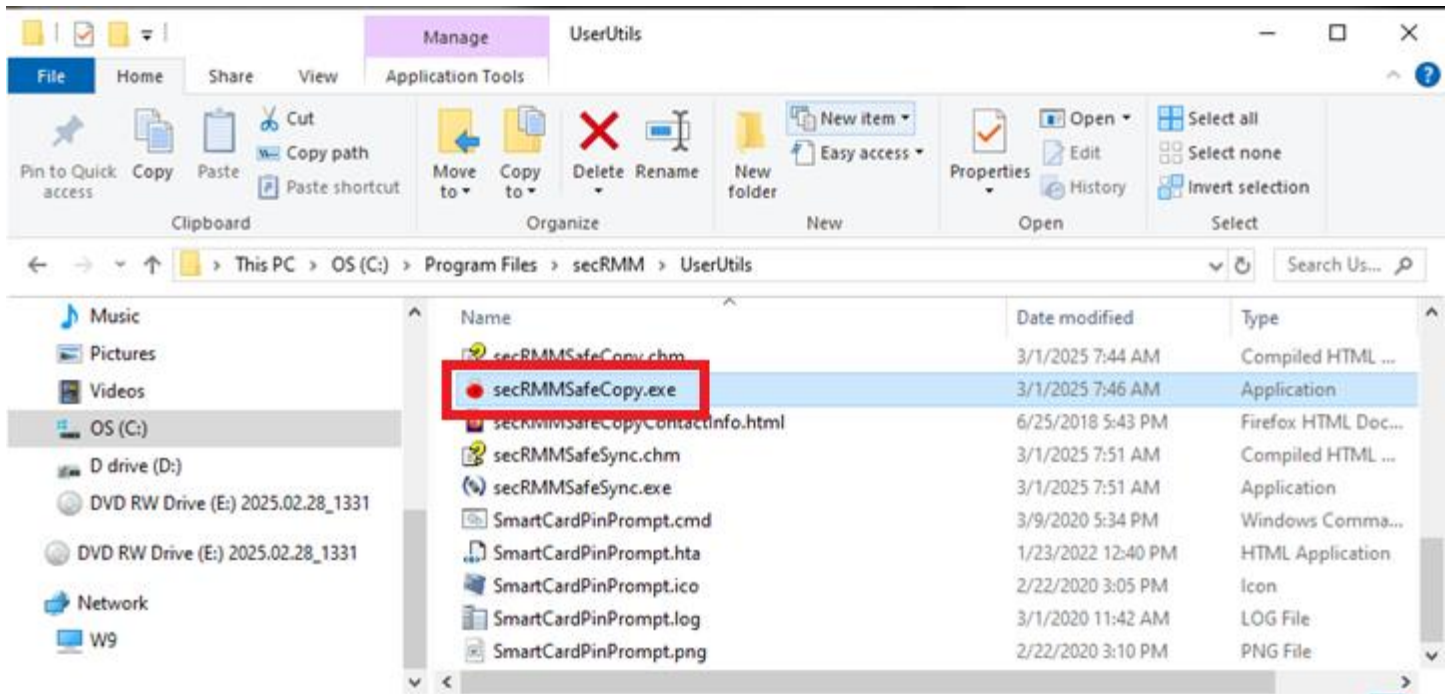


This document will reference the term "CD/DVD/Blu-ray discs" as just "discs" so the documentation is not cluttered with this long term.

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".

secRMM Administrator Guide



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. you 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)

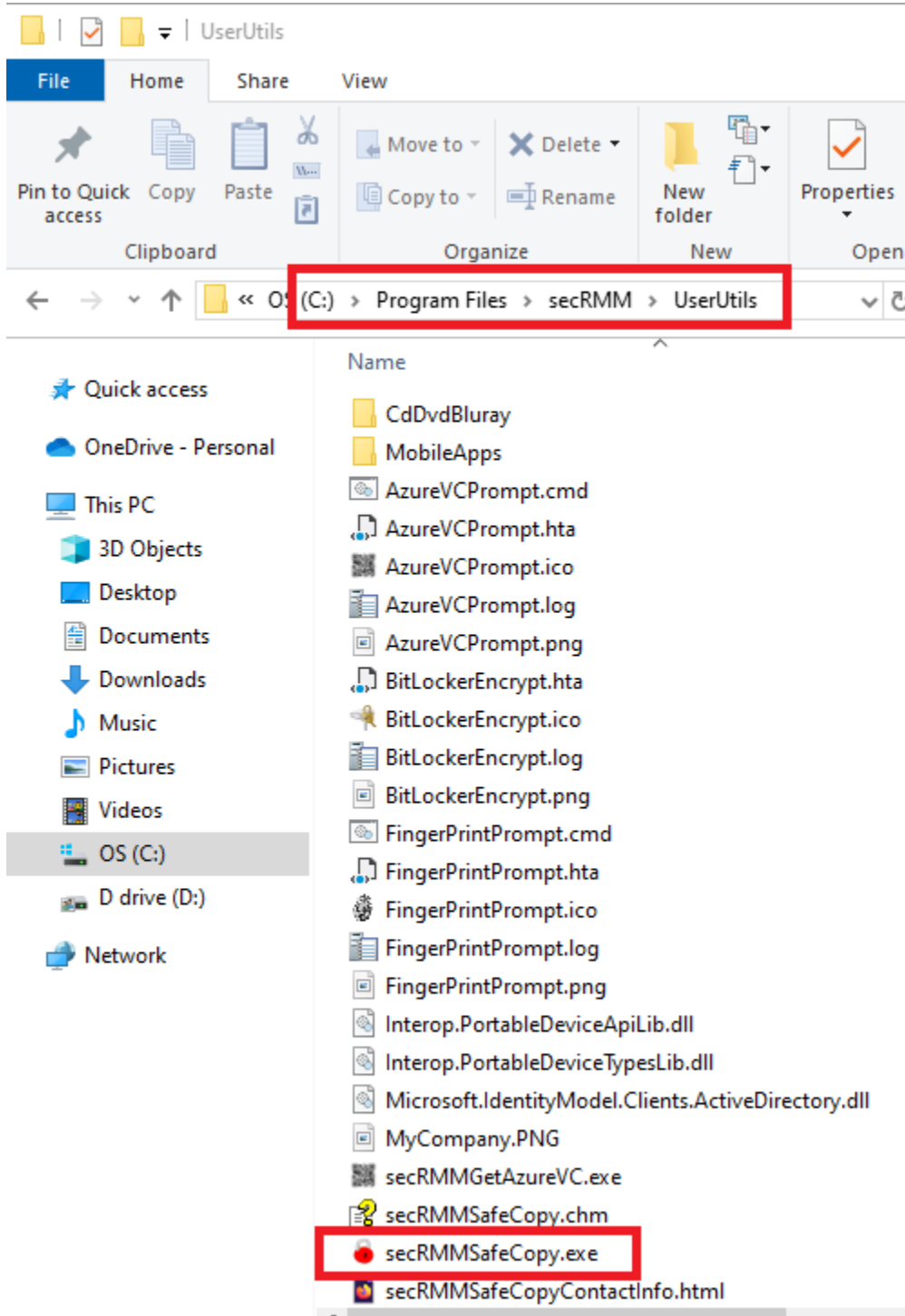
Create an encrypted disc

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

1. Start the secRMMSafeCopy program¹

¹ 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).

secRMM Administrator Guide



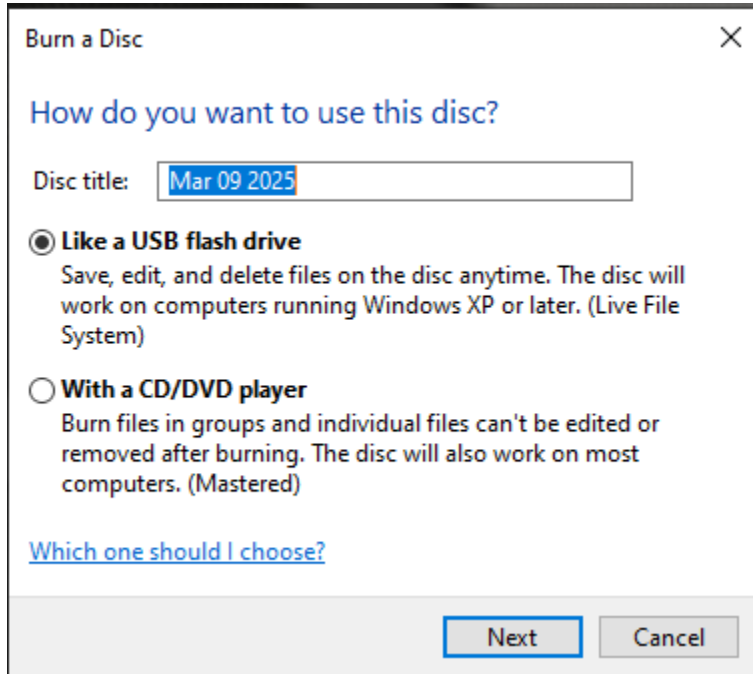
2. If you are using an external Cd/DVD/Blu-Ray drive, USB attach it to the Windows computer now



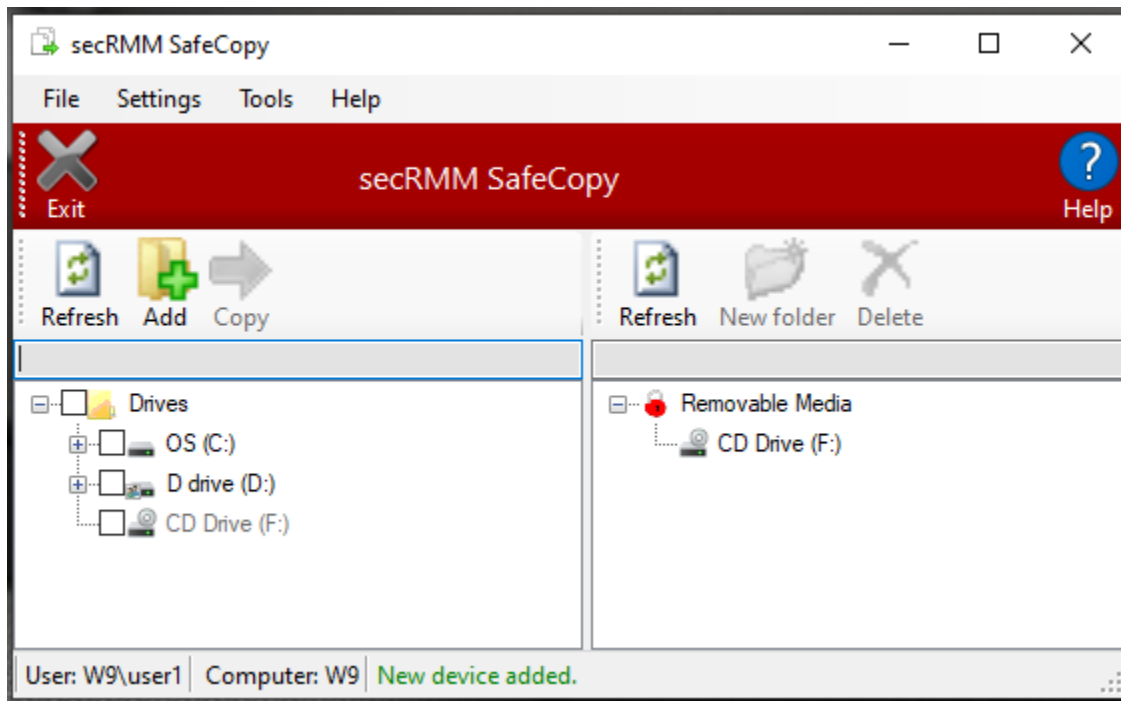
3. Insert a blank disc and close the door to the external drive.



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.

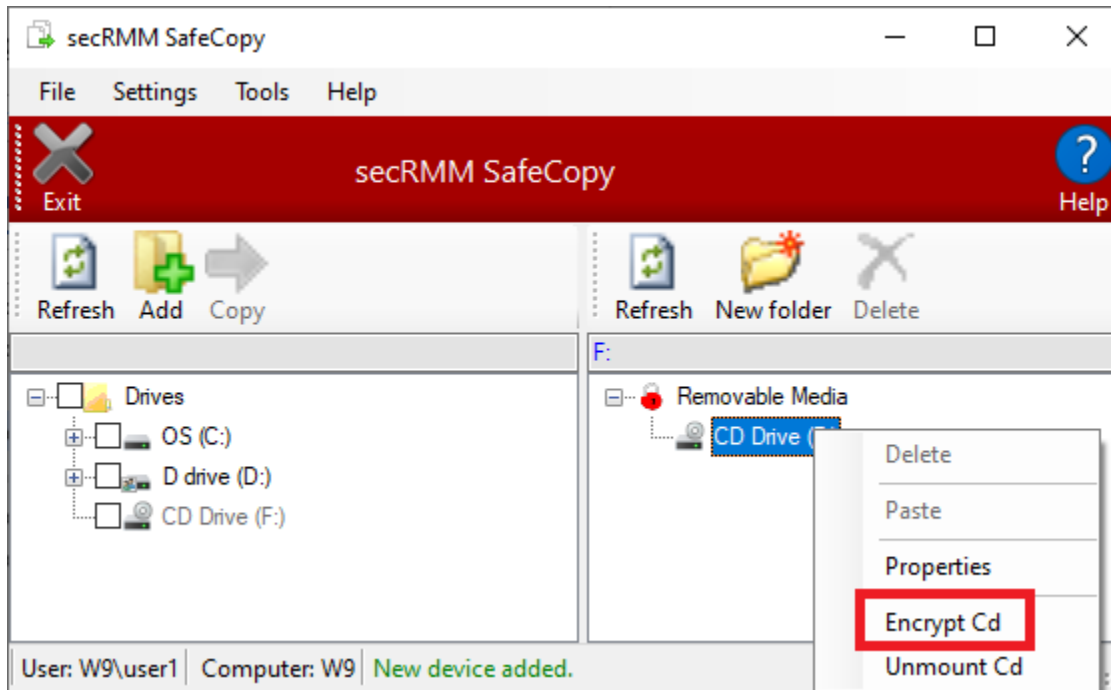


5. secRMMSafeCopy will see the blank disc. Note that the CD Drive will show up in both the left and right lists. The list on the left is what Windows sees (similar to Windows explorer) and the list on the right is what secRMM is monitoring/managing.



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

secRMM Encrypted CD/DVD/Blu-ray User Guide



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.

b. Folder where the data files are located

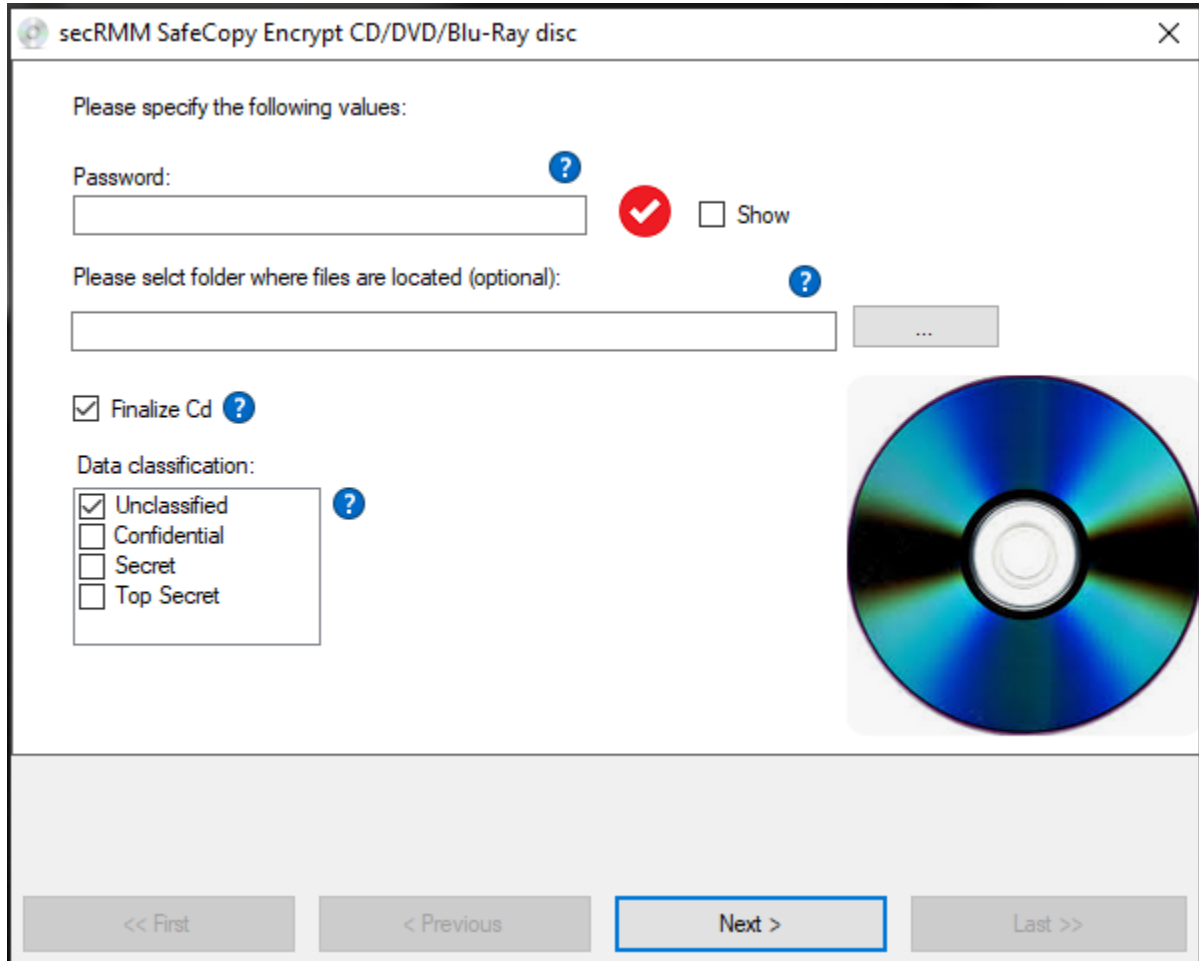
Note that there is a button to the right of this field that shows you the folders on your computer.

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 Administrator Guide

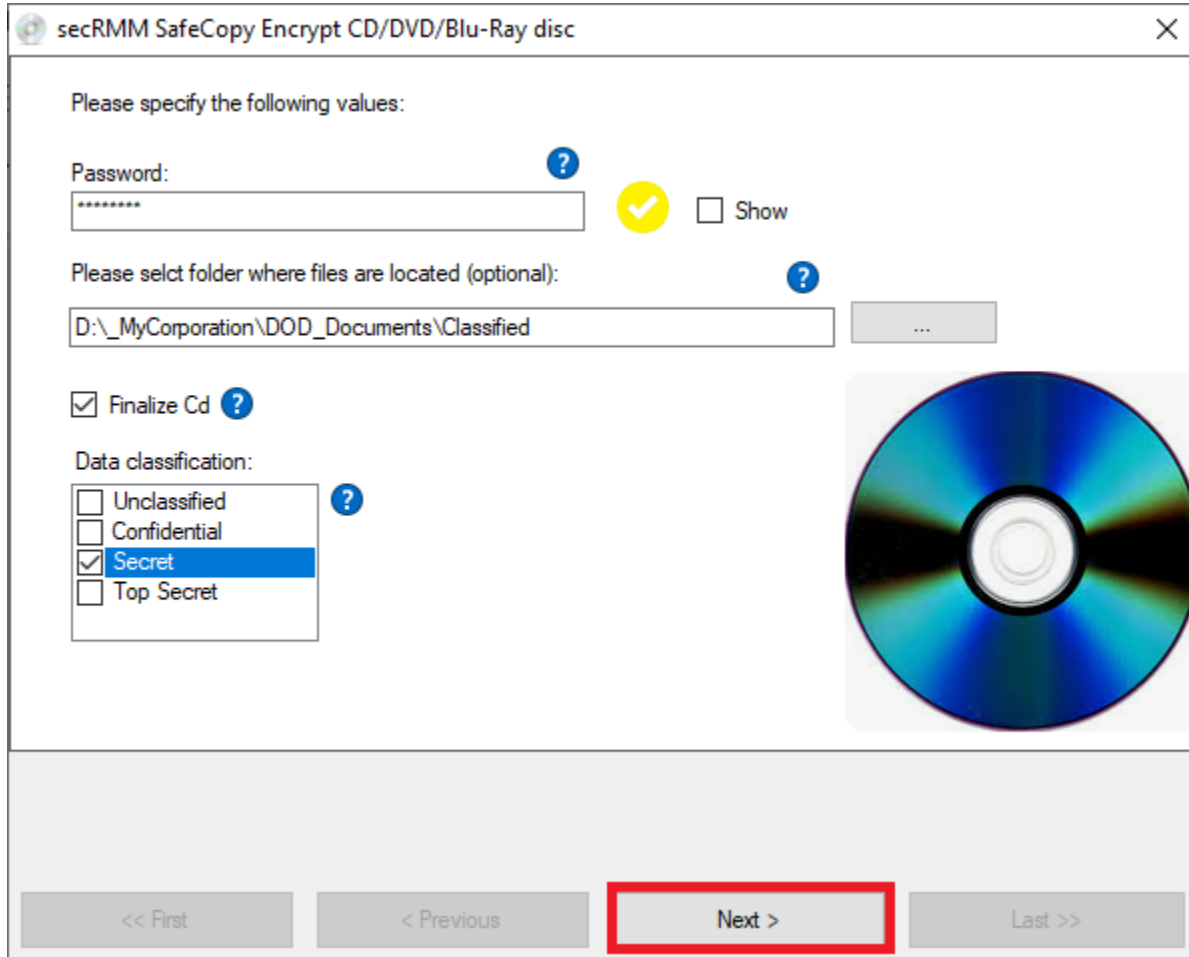


The screenshot shows a dialog box titled "secRMM SafeCopy Encrypt CD/DVD/Blu-Ray disc". The dialog contains the following elements:

- A header bar with the title and a close button (X).
- The instruction: "Please specify the following values:"
- A "Password:" label with a blue question mark icon, followed by a text input field, a red checkmark icon, and a "Show" checkbox.
- A "Please select folder where files are located (optional):" label with a blue question mark icon, followed by a text input field and a browse button with three dots.
- A "Finalize Cd" checkbox with a blue question mark icon, which is currently checked.
- A "Data classification:" label with a blue question mark icon, followed by a list of four options: "Unclassified" (checked), "Confidential", "Secret", and "Top Secret".
- A large image of a CD/DVD disc on the right side.
- A footer bar with four navigation buttons: "<< First", "< Previous", "Next >" (highlighted with a blue border), and "Last >>".

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

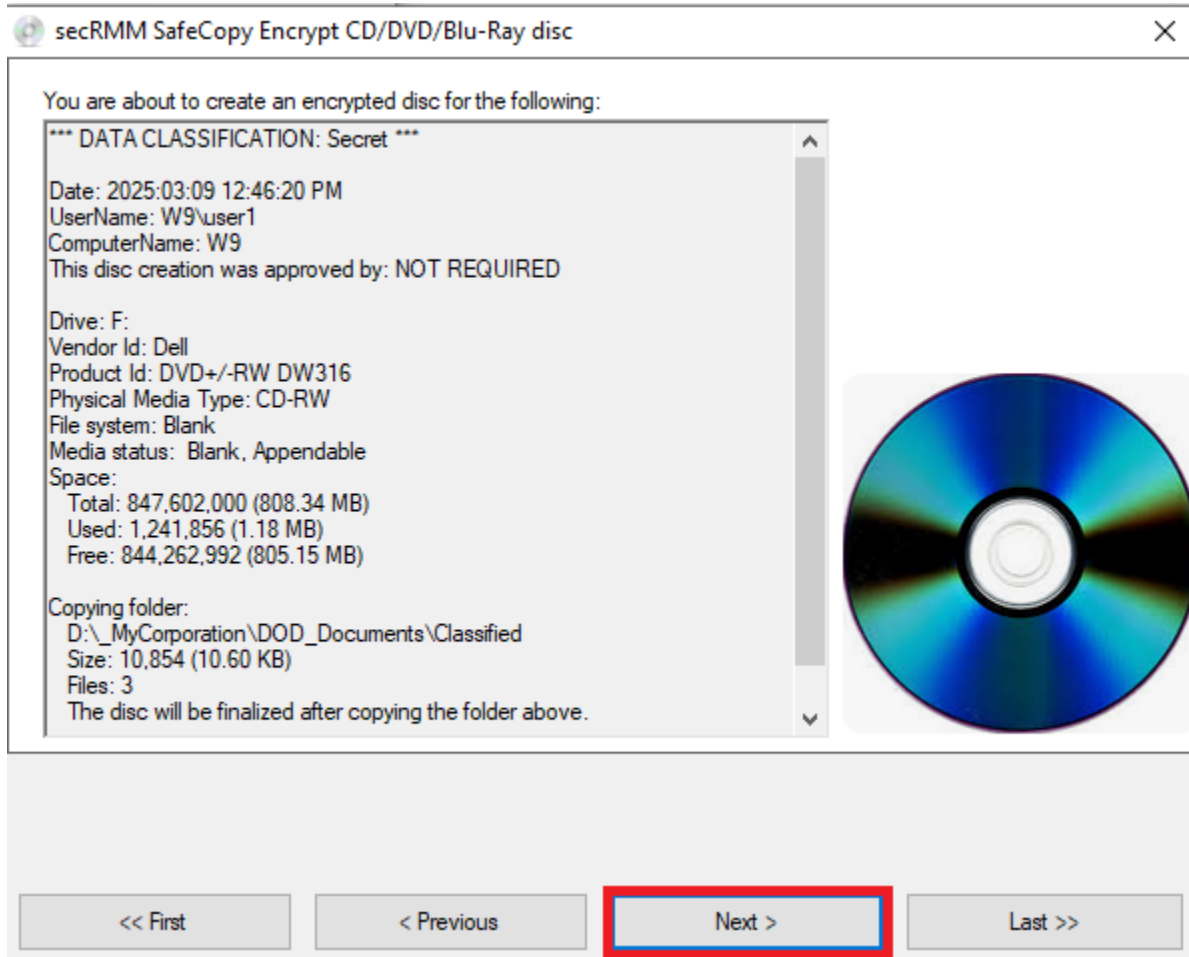
secRMM Encrypted CD/DVD/Blu-ray User Guide



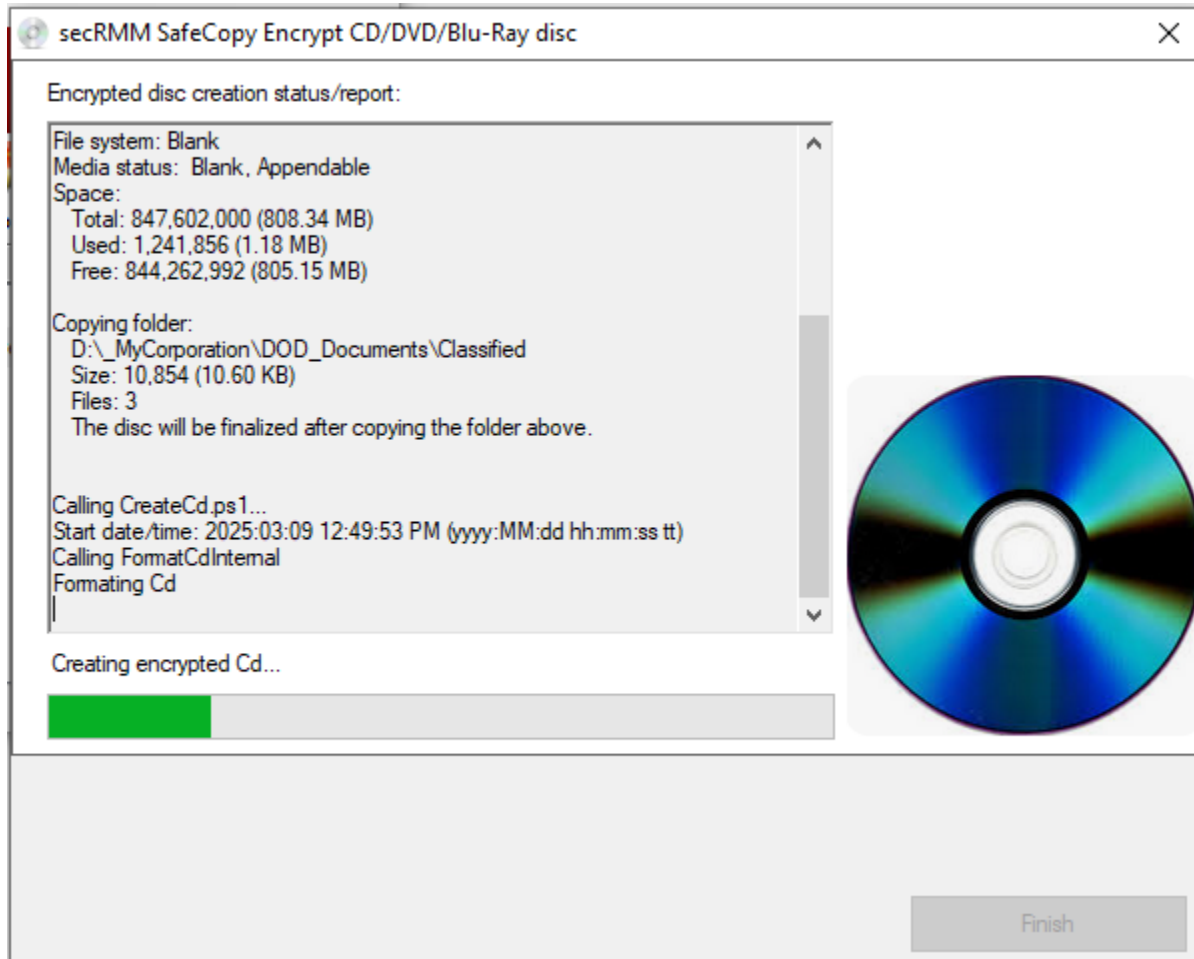
The screenshot shows a dialog box titled "secRMM SafeCopy Encrypt CD/DVD/Blu-Ray disc". The dialog contains the following elements:

- A header bar with a close button (X) in the top right corner.
- The instruction: "Please specify the following values:"
- A "Password:" label with a question mark icon. Below it is a text input field containing "*****". To the right of the field is a yellow checkmark icon and a "Show" checkbox.
- A "Please select folder where files are located (optional):" label with a question mark icon. Below it is a text input field containing "D:_MyCorporation\DOD_Documents\Classified" and a browse button with three dots.
- A checked checkbox labeled "Finalize Cd" with a question mark icon.
- A "Data classification:" label with a question mark icon. Below it is a list box with four options: "Unclassified", "Confidential", "Secret", and "Top Secret". The "Secret" option is selected and highlighted in blue.
- A large image of a blue CD/DVD disc on the right side of the dialog.
- A footer bar with four navigation buttons: "<< First", "< Previous", "Next >", and "Last >>". The "Next >" button is highlighted with a red rectangular border.

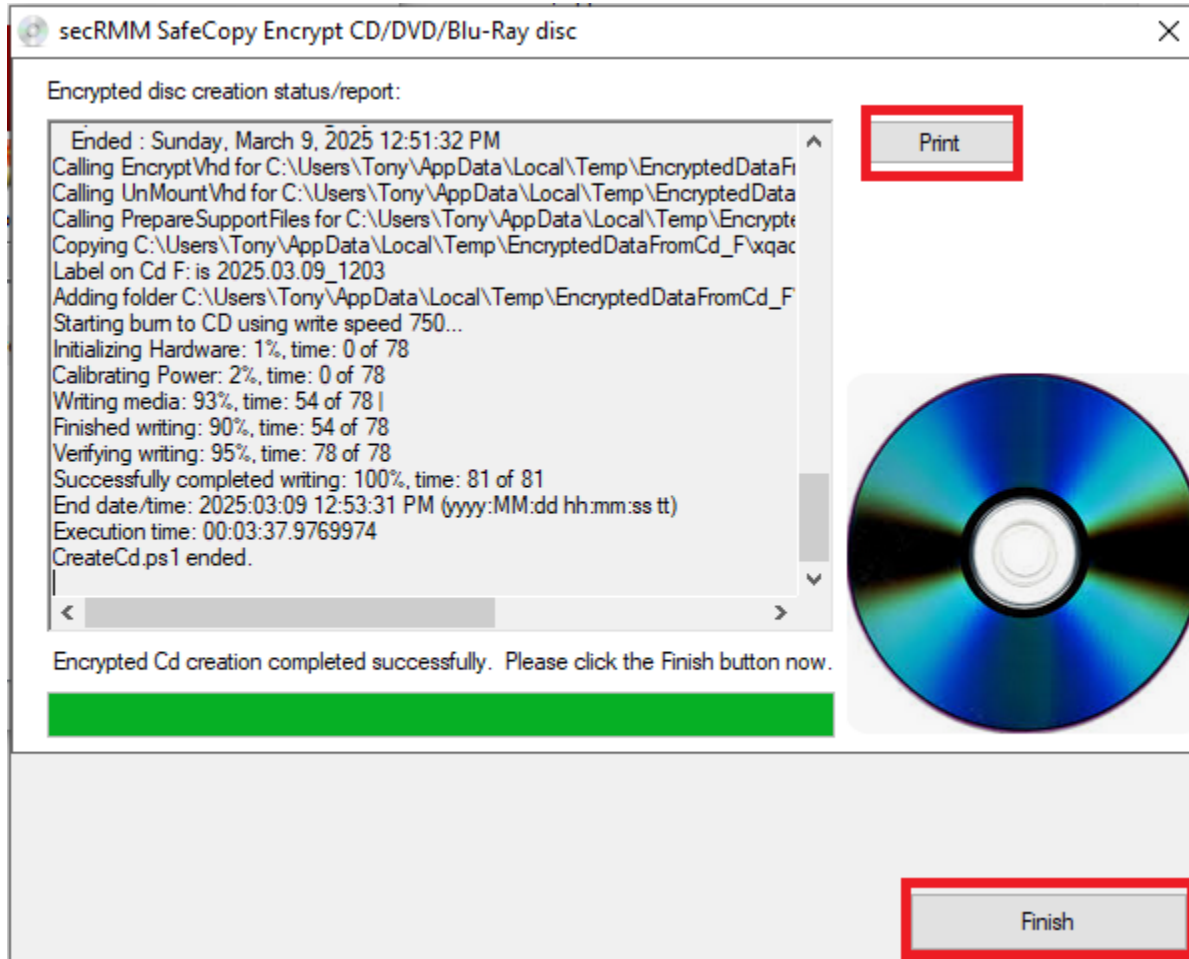
8. You can now review the information about this encrypted disc creation. If you are satisfied with the information, you can click the 'Next' button or go back to make any changes by clicking the 'Previous' button.



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.



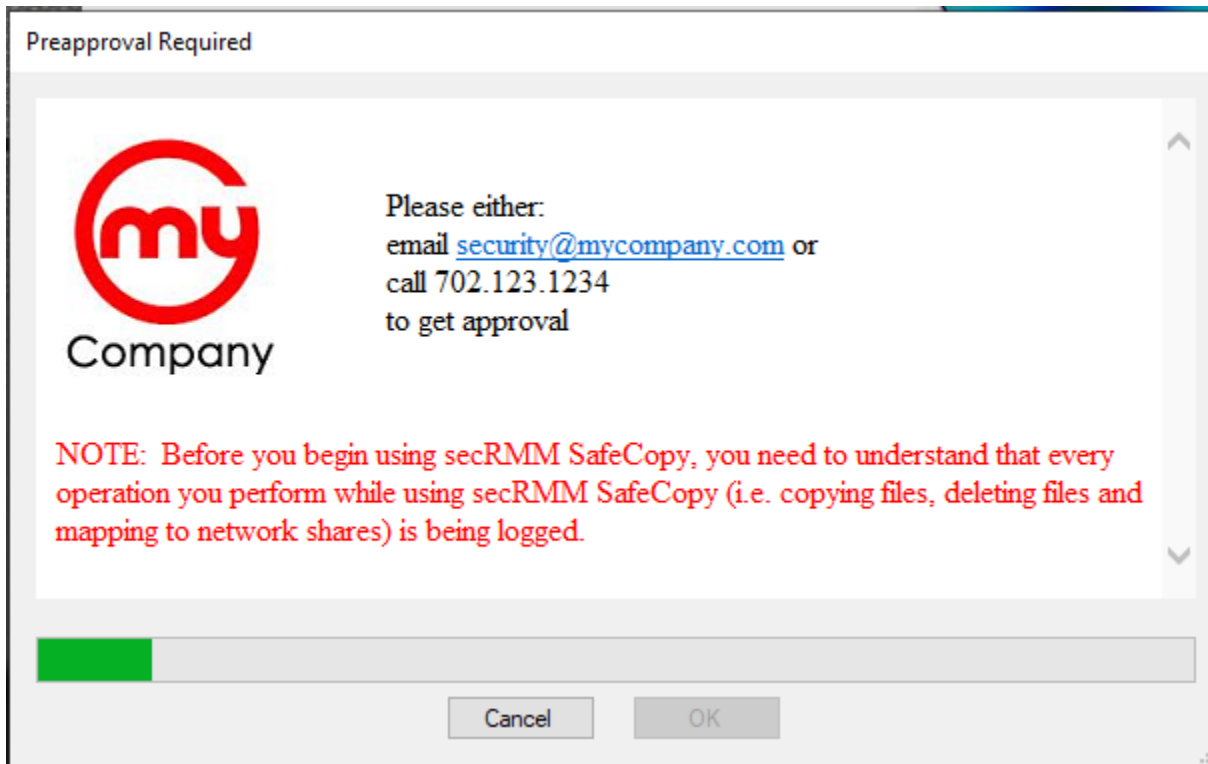
10. Once the encrypted disc is created:
 - a. The Finish button will become enabled
 - b. A print button will become visible so you can print the status/report (optional)
 - c. The newly created encrypted disc will eject from the disc drive



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".

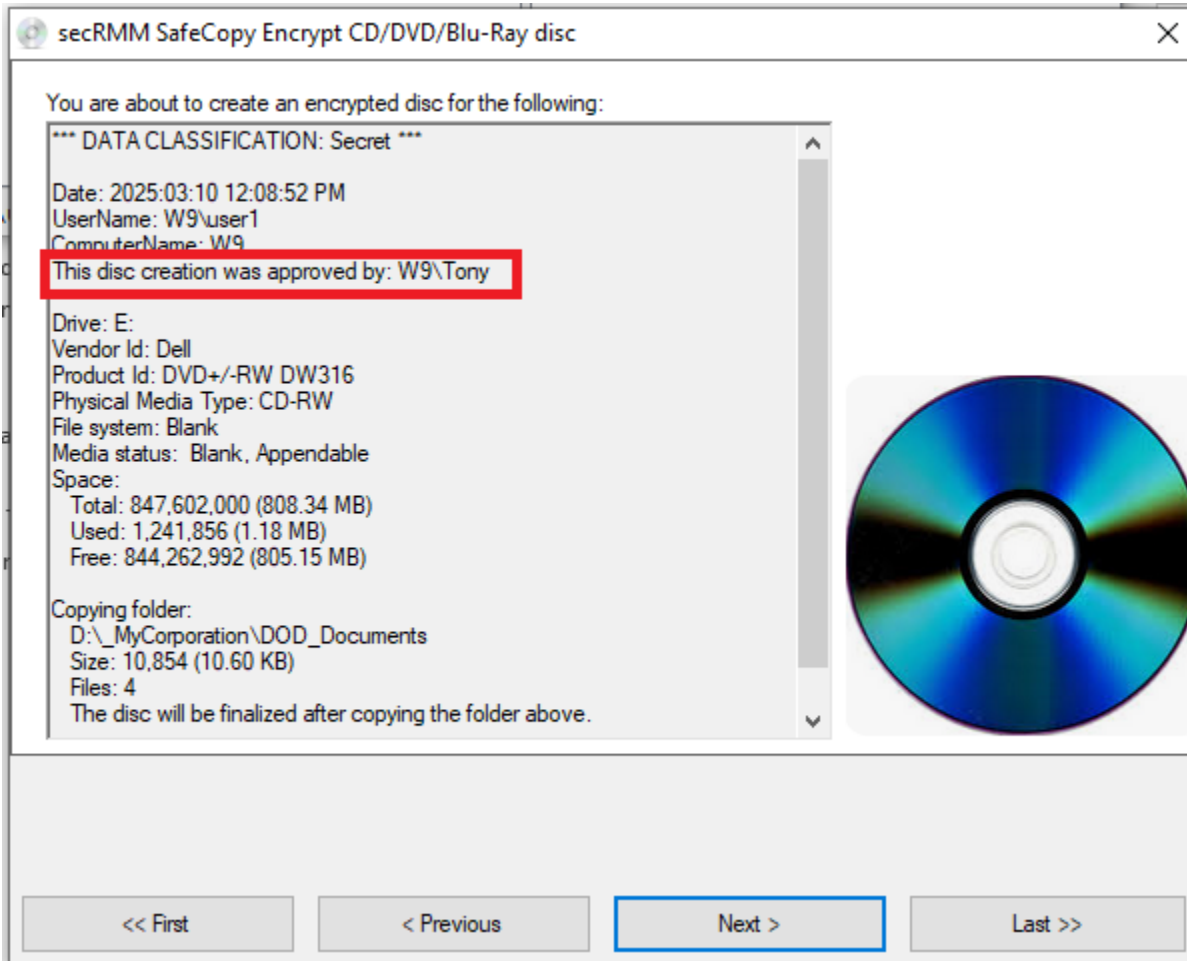
Preapproval (two man policy)

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.

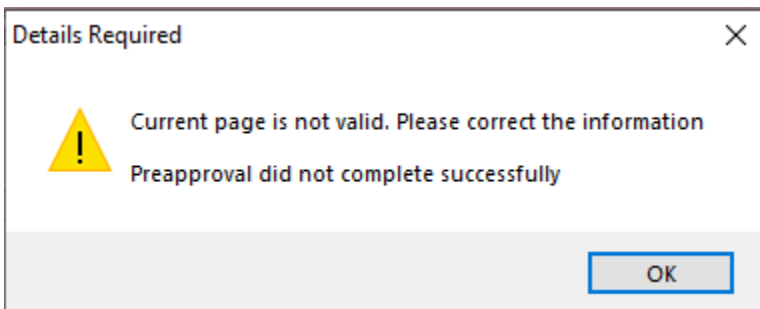
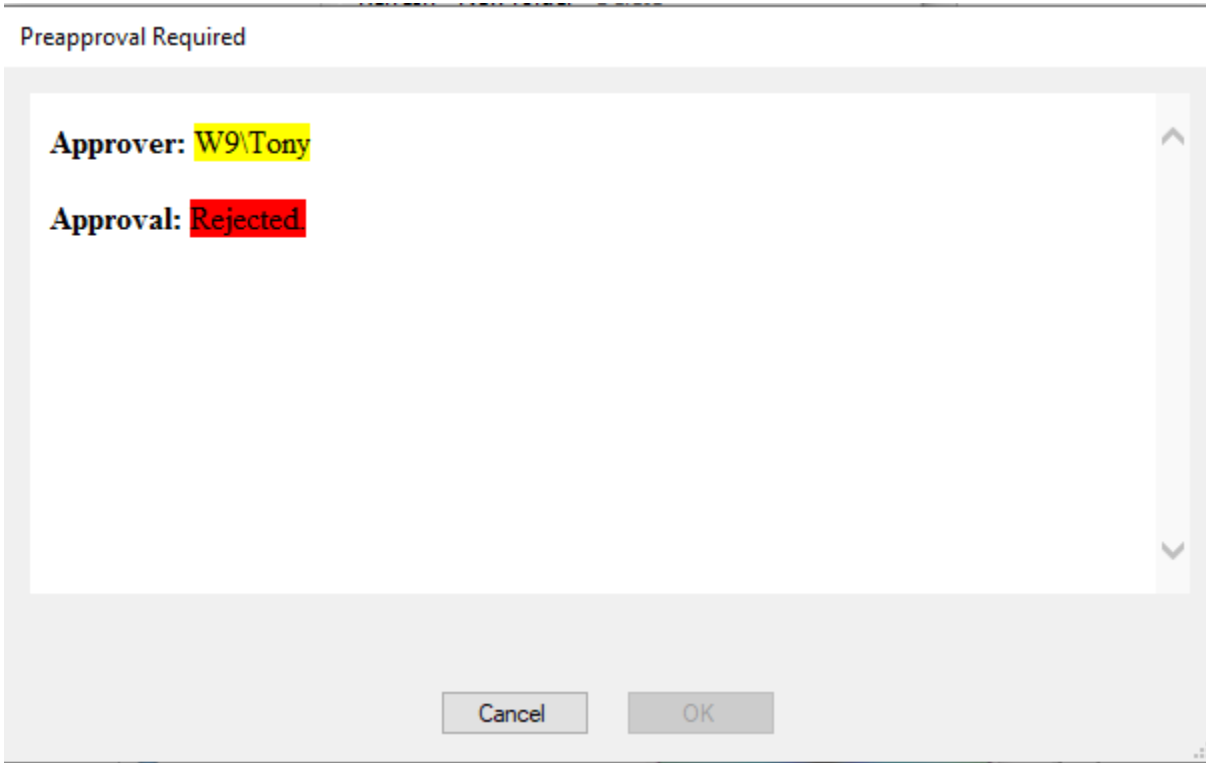


Once the approval process has been performed, you can continue creating the encrypted disc following the steps above. Note that the status/report will show who approved the creation of the encrypted disc as shown in the screenshot below.

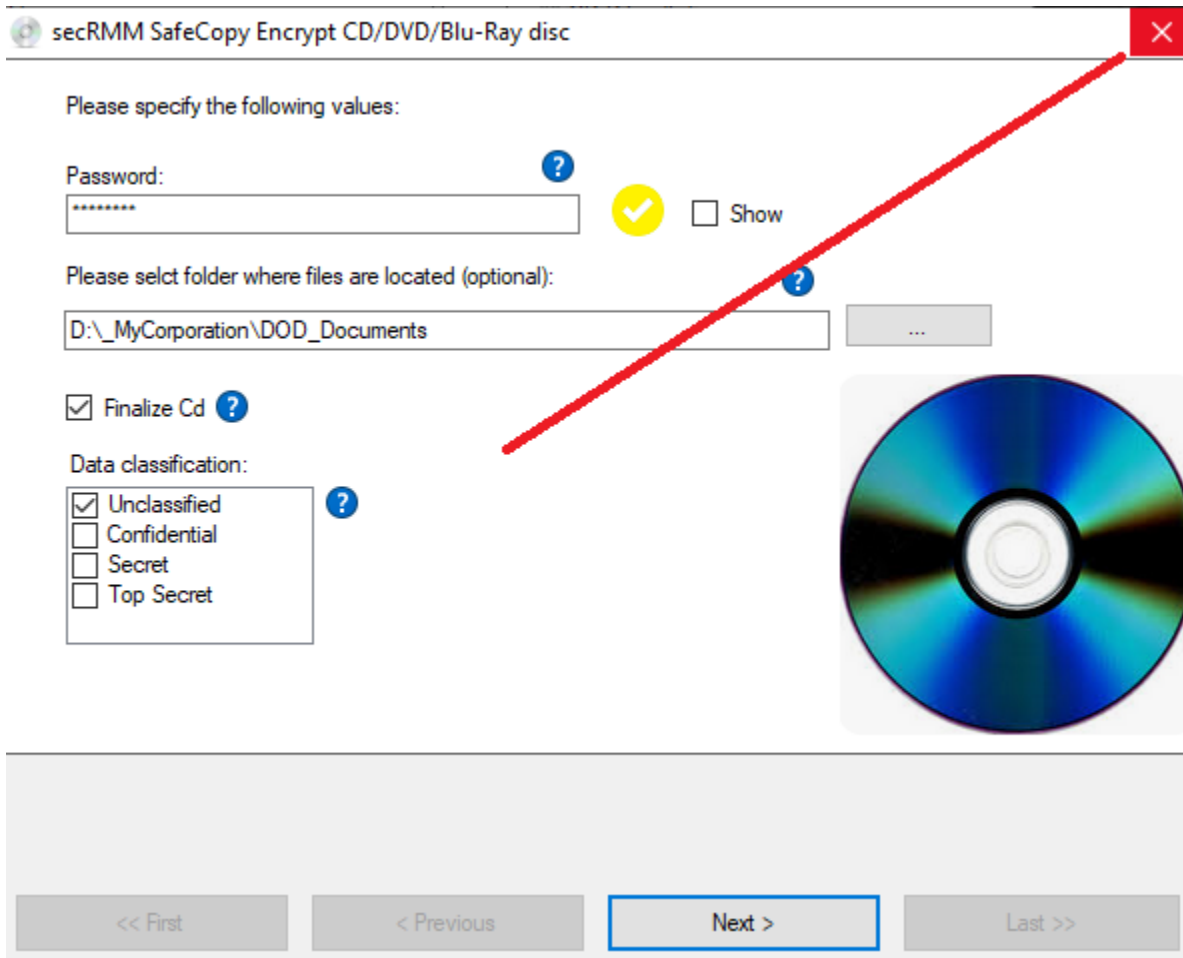
secRMM Administrator Guide



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.



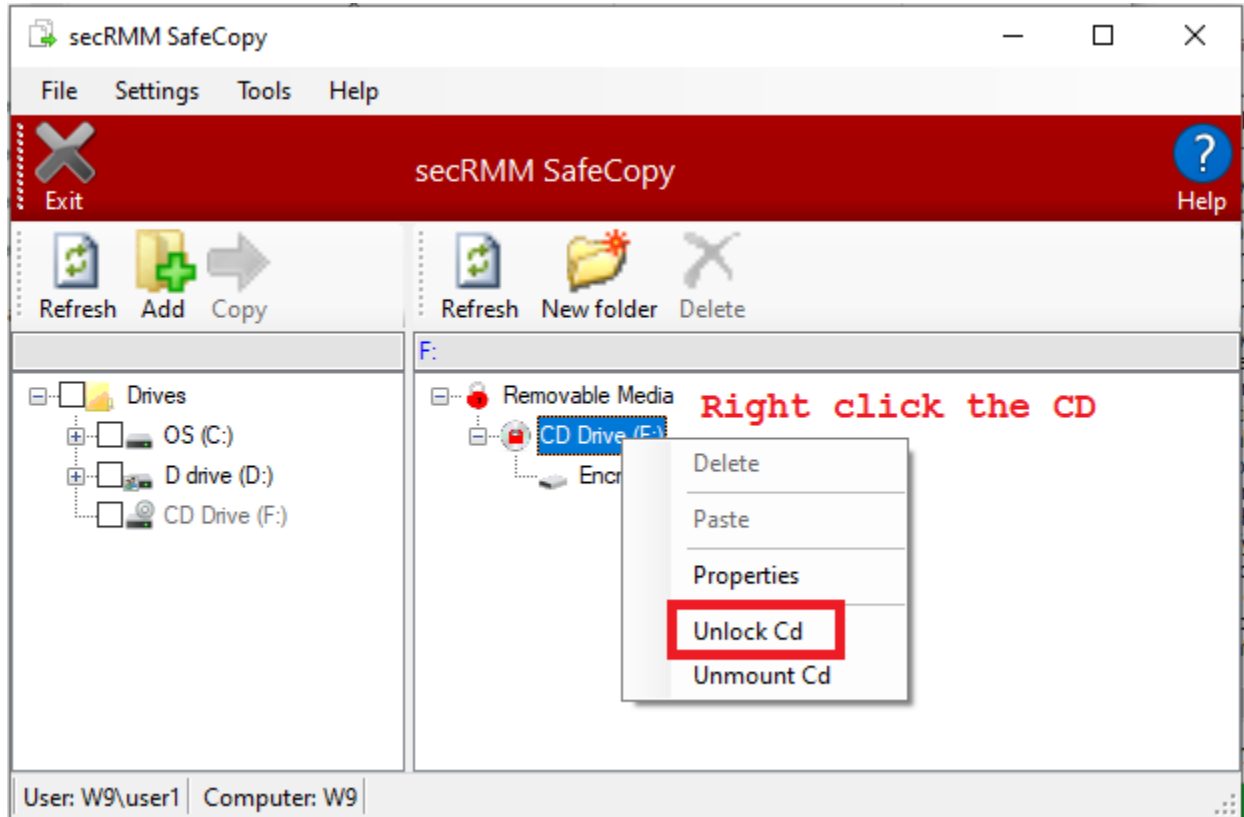
You must click the close button (as shown in the screenshot below) until you can get proper approval to create an encrypted disc.



Unlock an encrypted disc

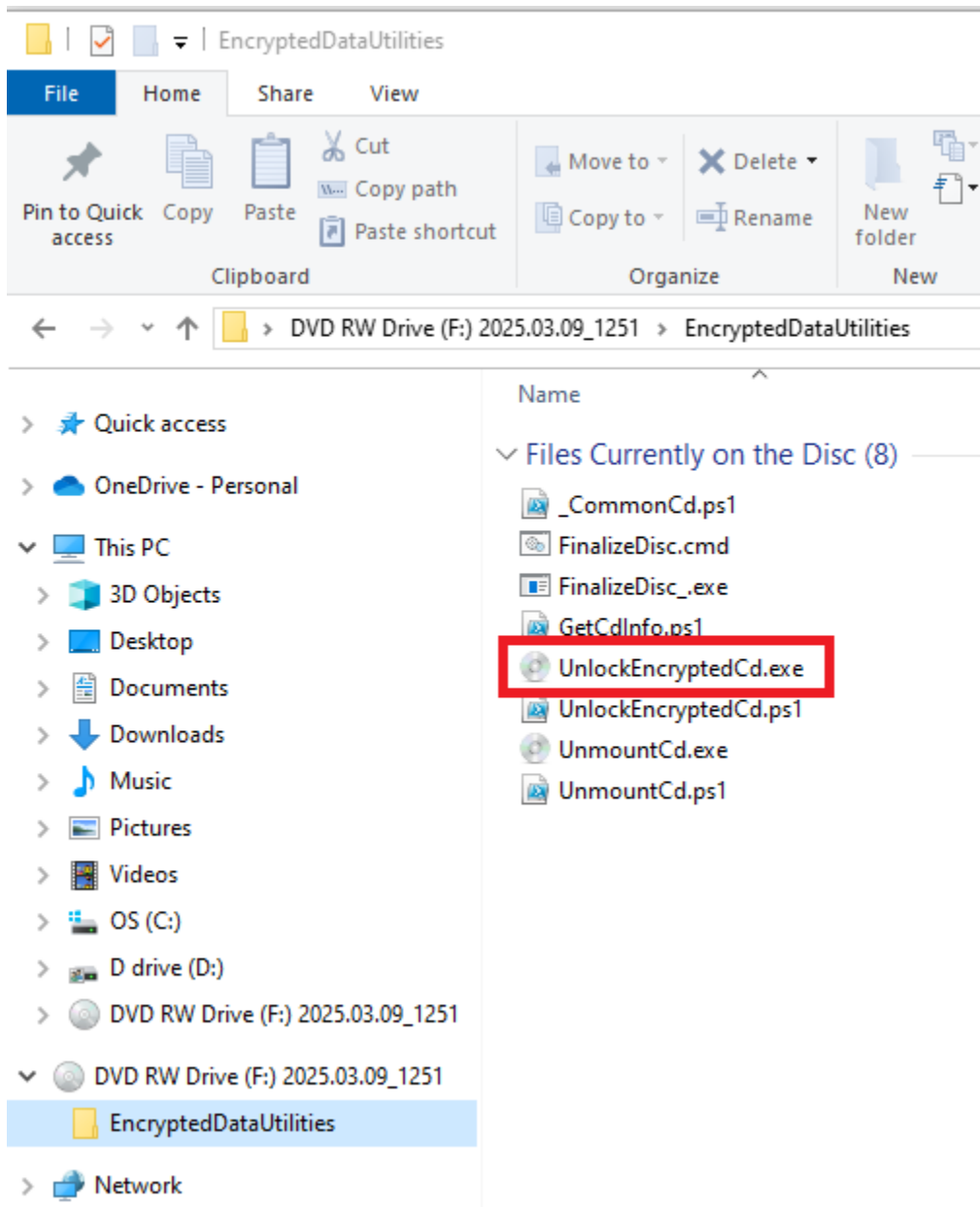
Please follow the steps and screenshots in this section to unlock an encrypted disc. There are 3 ways to unlock an encrypted disc created by secRMMSafeCopy:

1. Use secRMMSafeCopy



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.

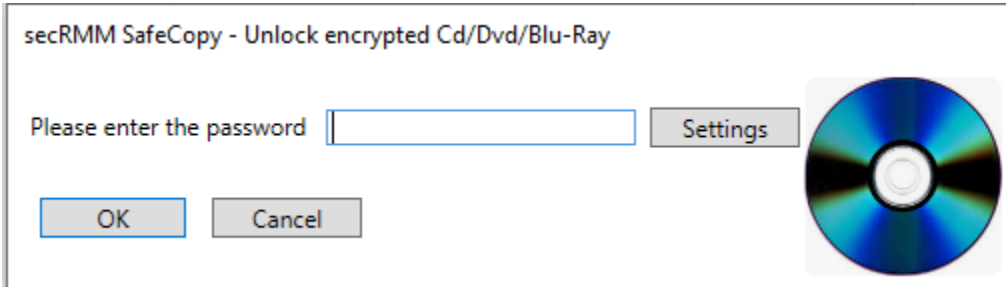
secRMM Administrator Guide



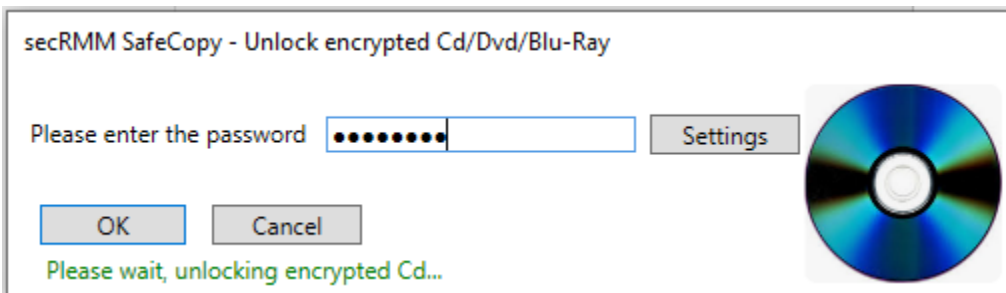
All 3 options above will display the UnlockEncryptedCd program as shown below. Provide the password used to create the encrypted disc. Please note there is no way to recover the password if you forget it².

² Please see the section below titled 'Overriding Enable-BitLocker' that describes how to create a recovery key in case of a forgotten password.

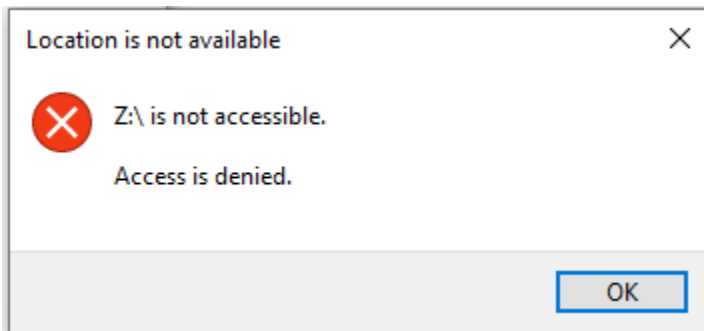
secRMM Encrypted CD/DVD/Blu-ray User Guide



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.

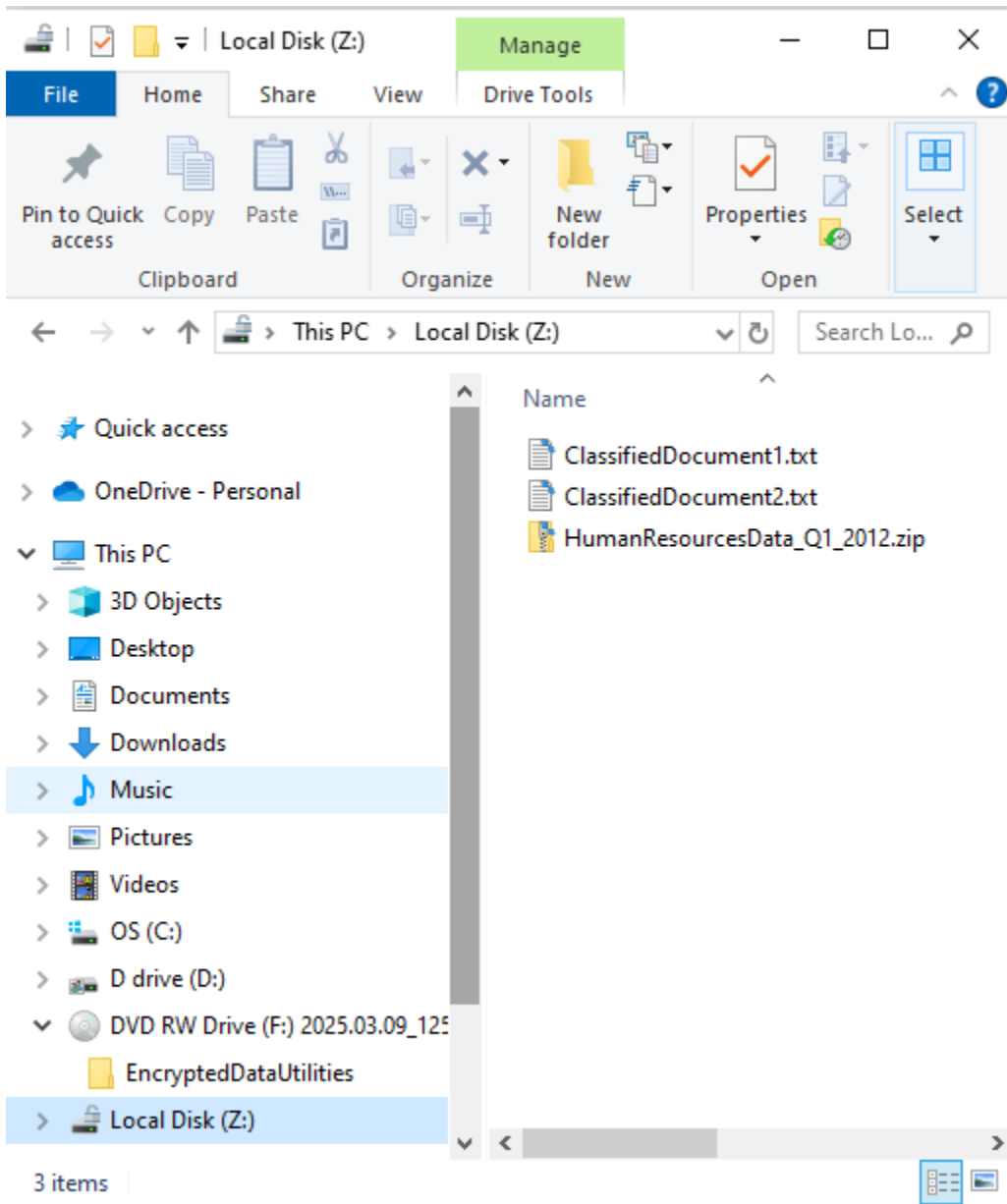
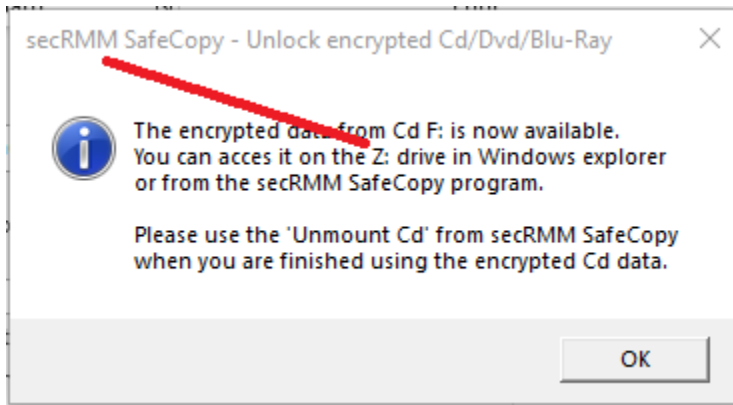


You will most likely get a pop-up message box from Windows explorer telling you 'Access is denied'. This is a timing issue/bug between BitLocker and Windows Explorer. You can simply click the OK button to dismiss it. We are working on a way to fix this annoying issue/bug.



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 Administrator Guide



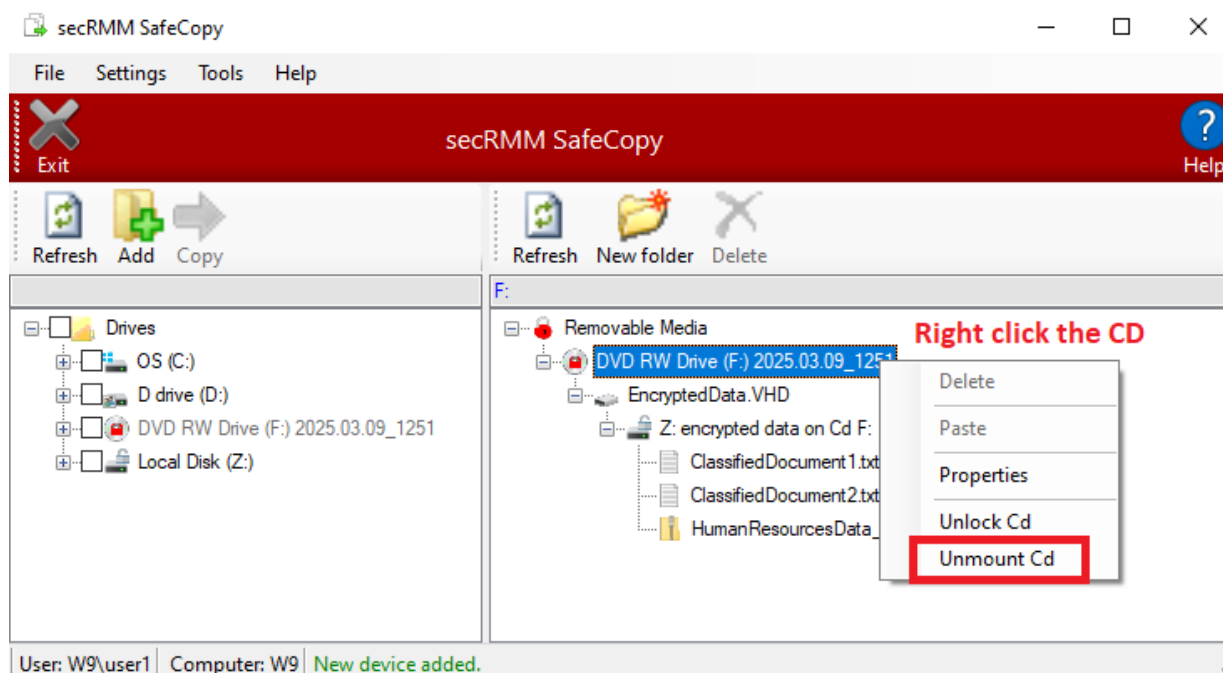
secRMM Encrypted CD/DVD/Blu-ray User Guide

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

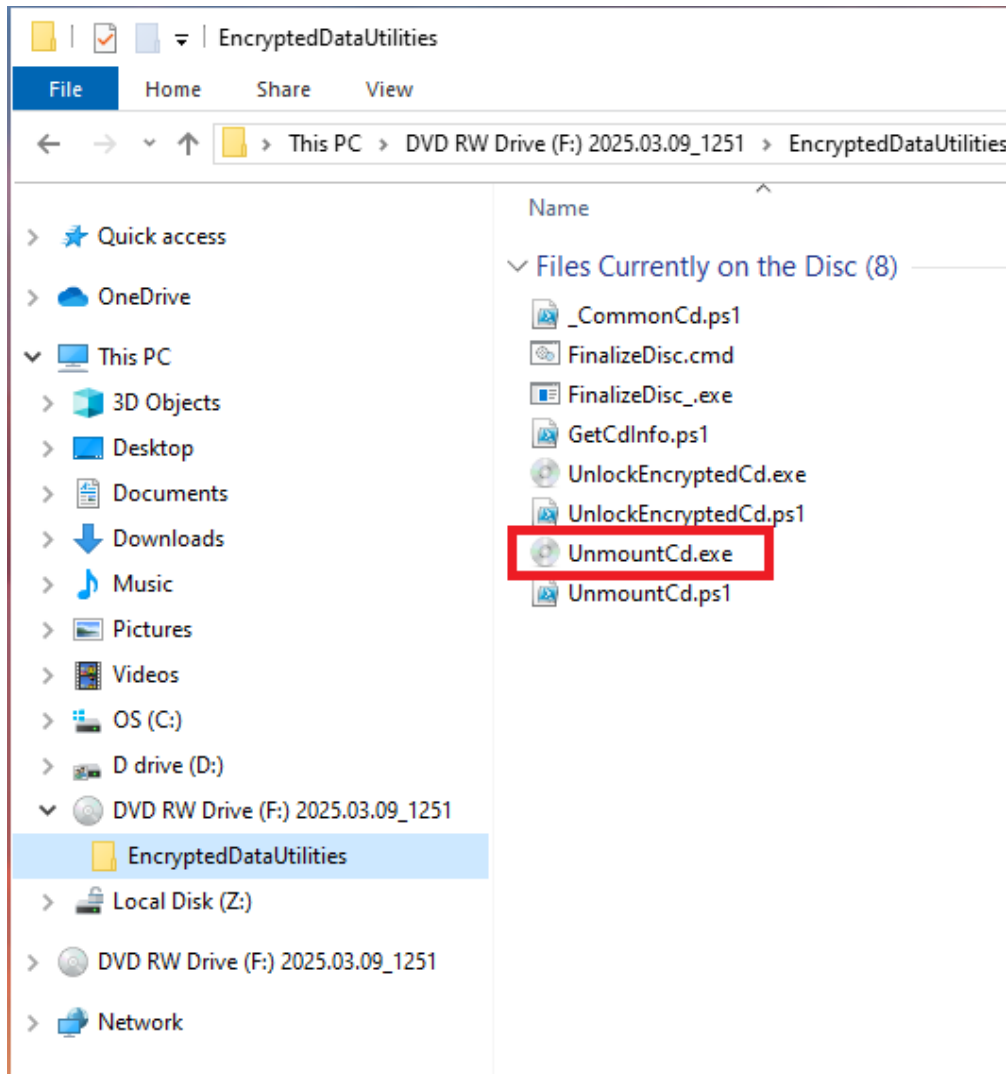
Please follow the steps and screenshots in this section to unmount an encrypted disc. There are 3 ways to unmount an encrypted disc created by secRMMSafeCopy:

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



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



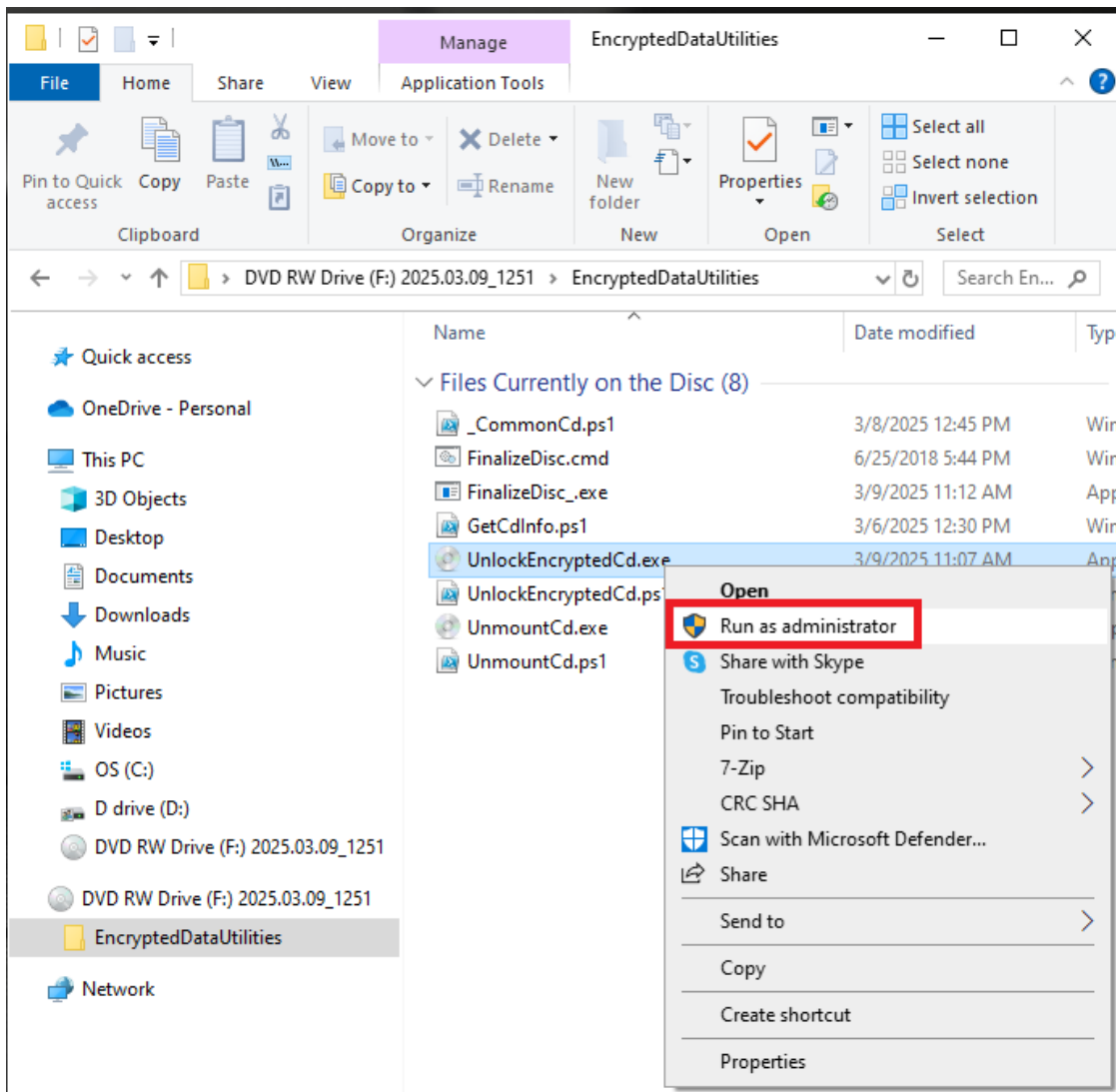
For most use cases, you will ignore the 2 checkboxes on this screen and simply click the OK button. The unmount will remove the temporary drive where the encrypted data was and eject the Cd drive.

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

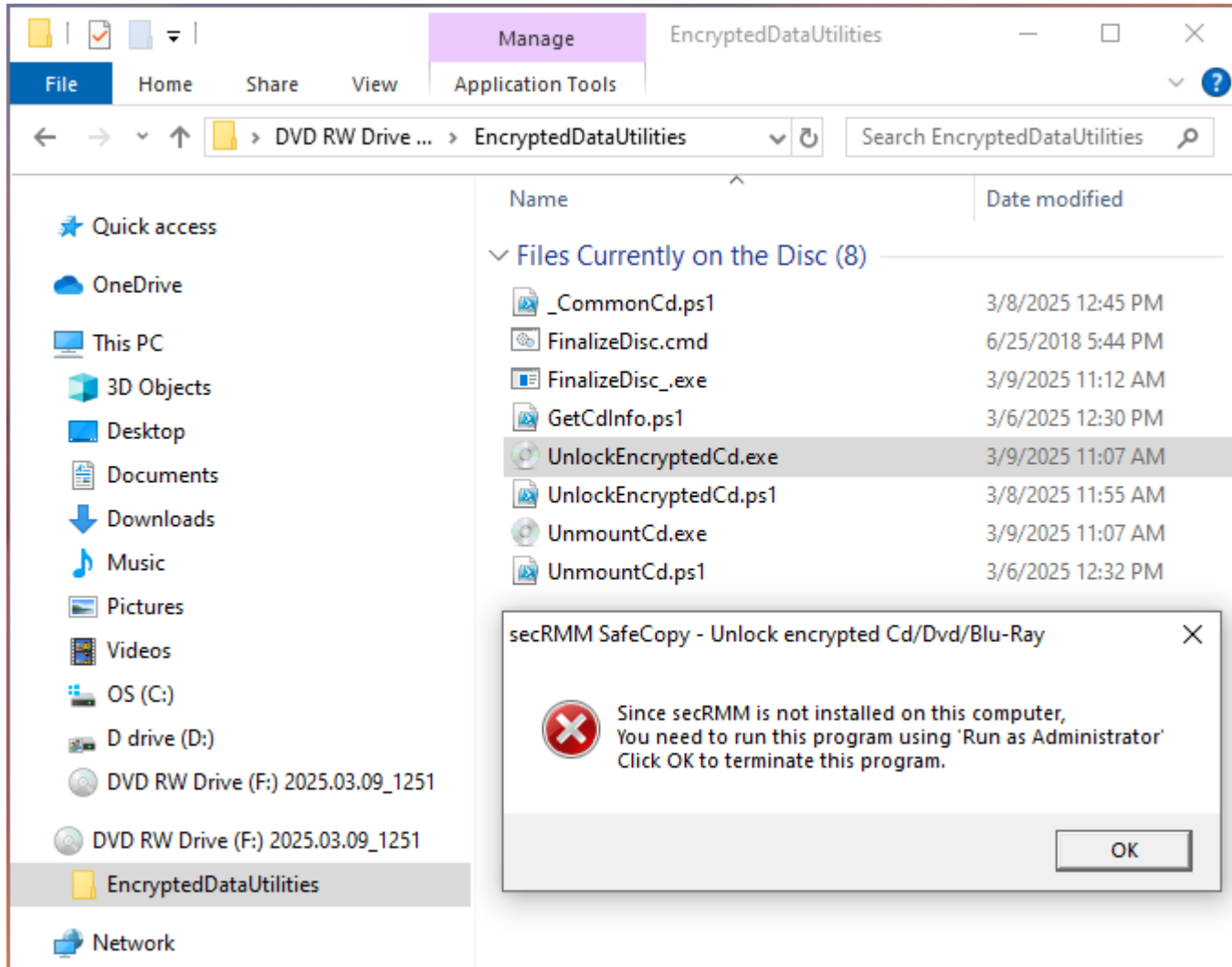
Using the secRMM provided programs on the disc

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').



secRMM Administrator Guide

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



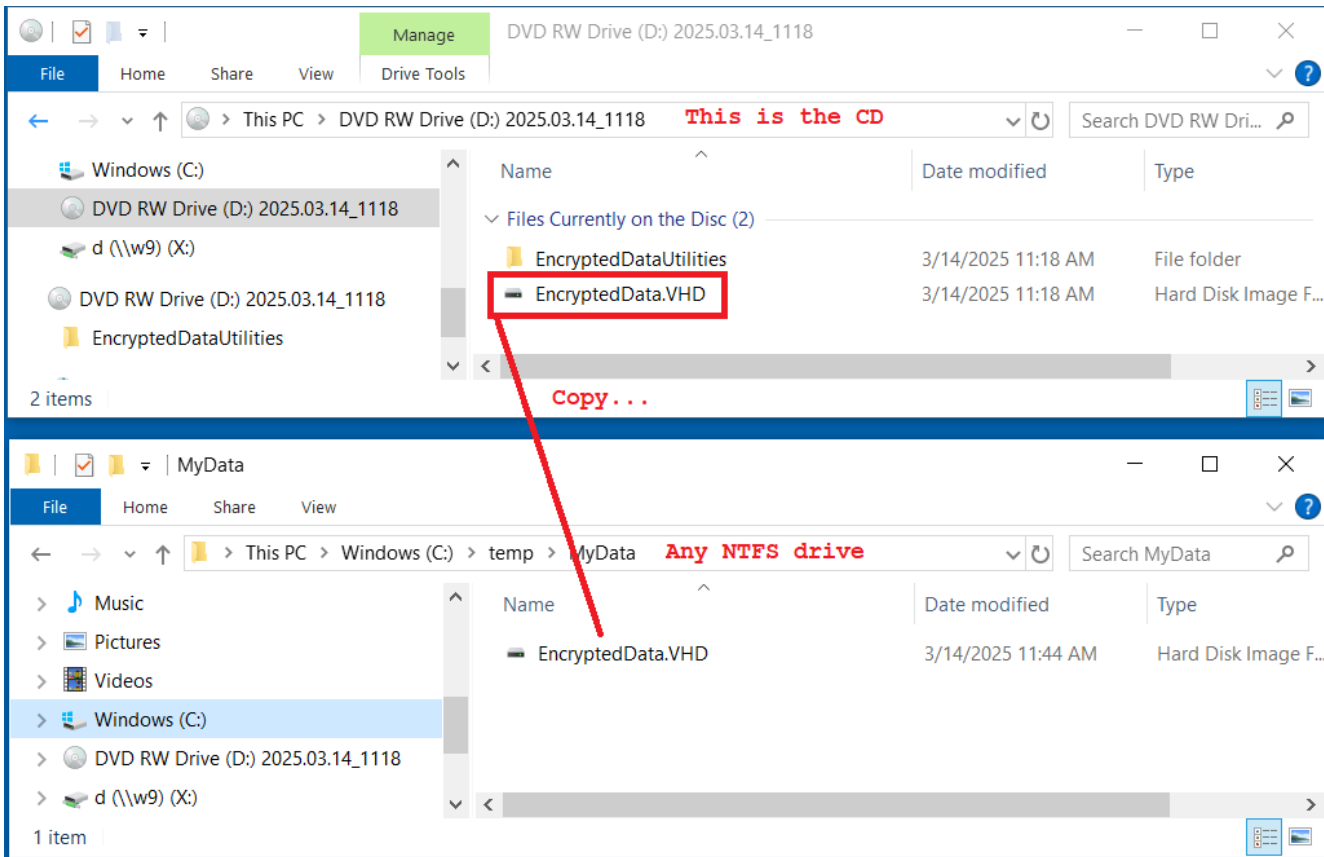
Using Windows Explorer

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.

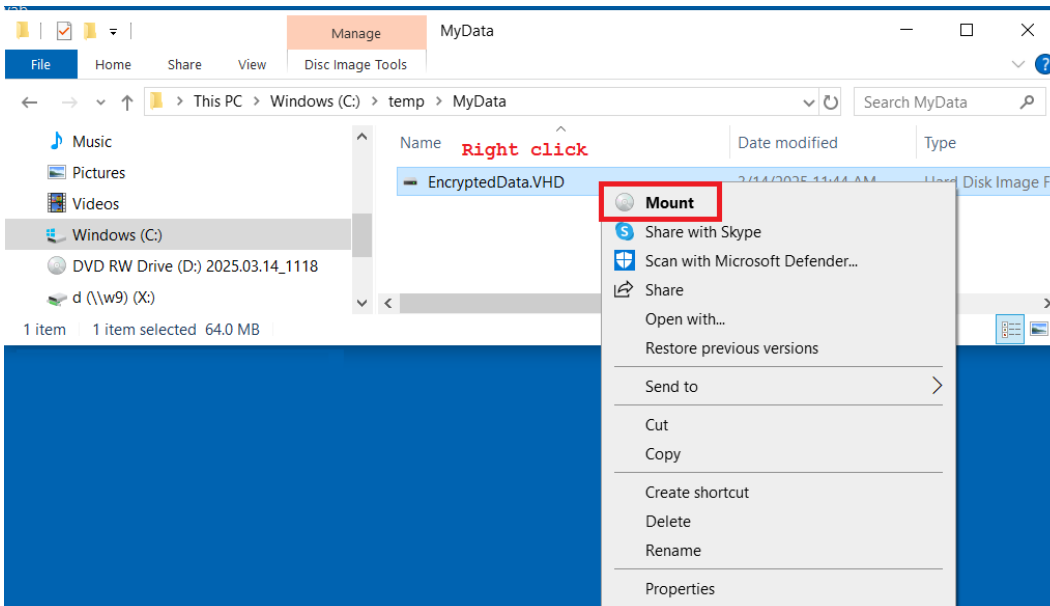
Unlock an encrypted disc

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



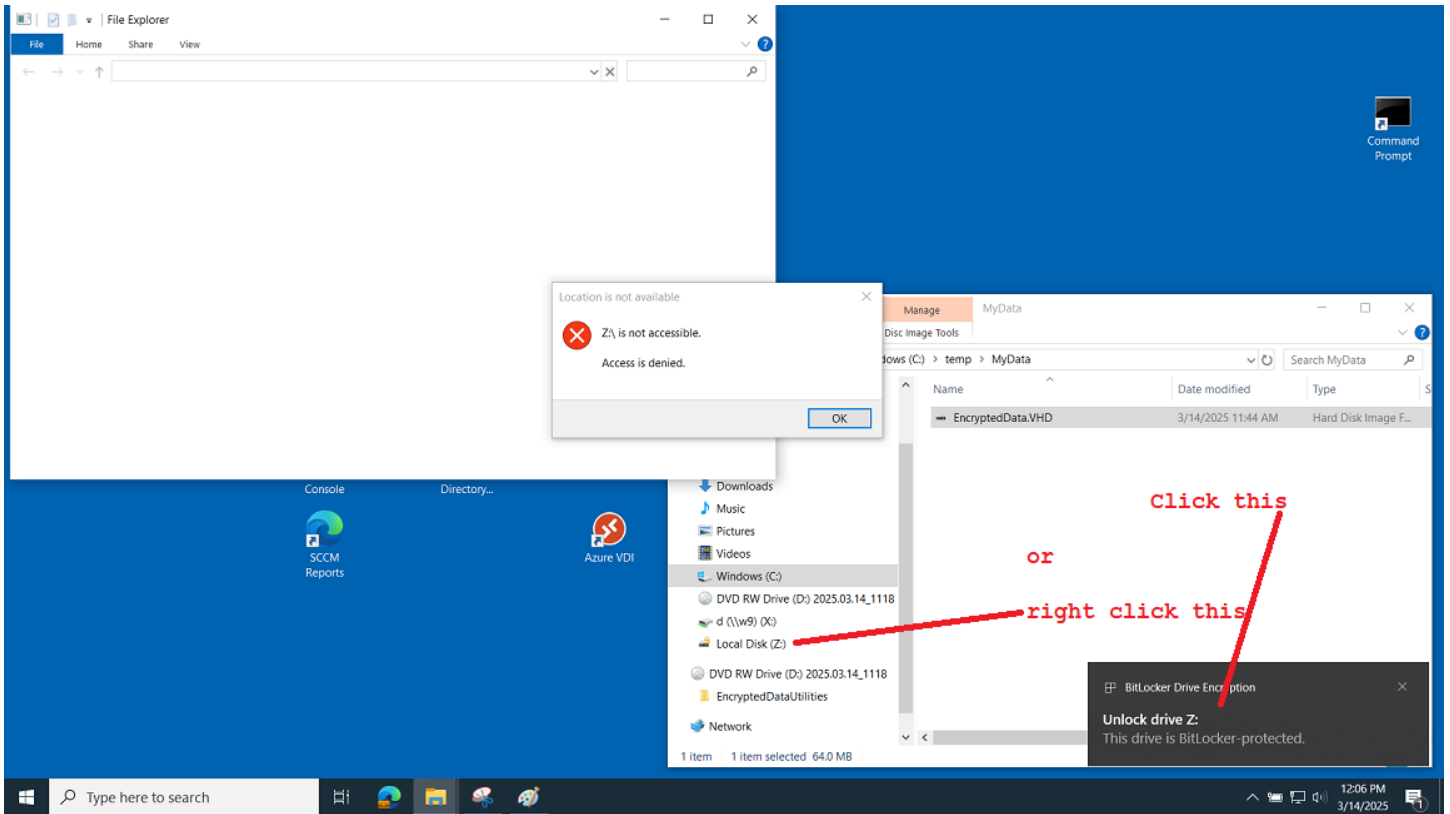
Right mouse click on the "EncryptedData.VHD" file (that you just copied to the NTFS drive). Select "Mount".

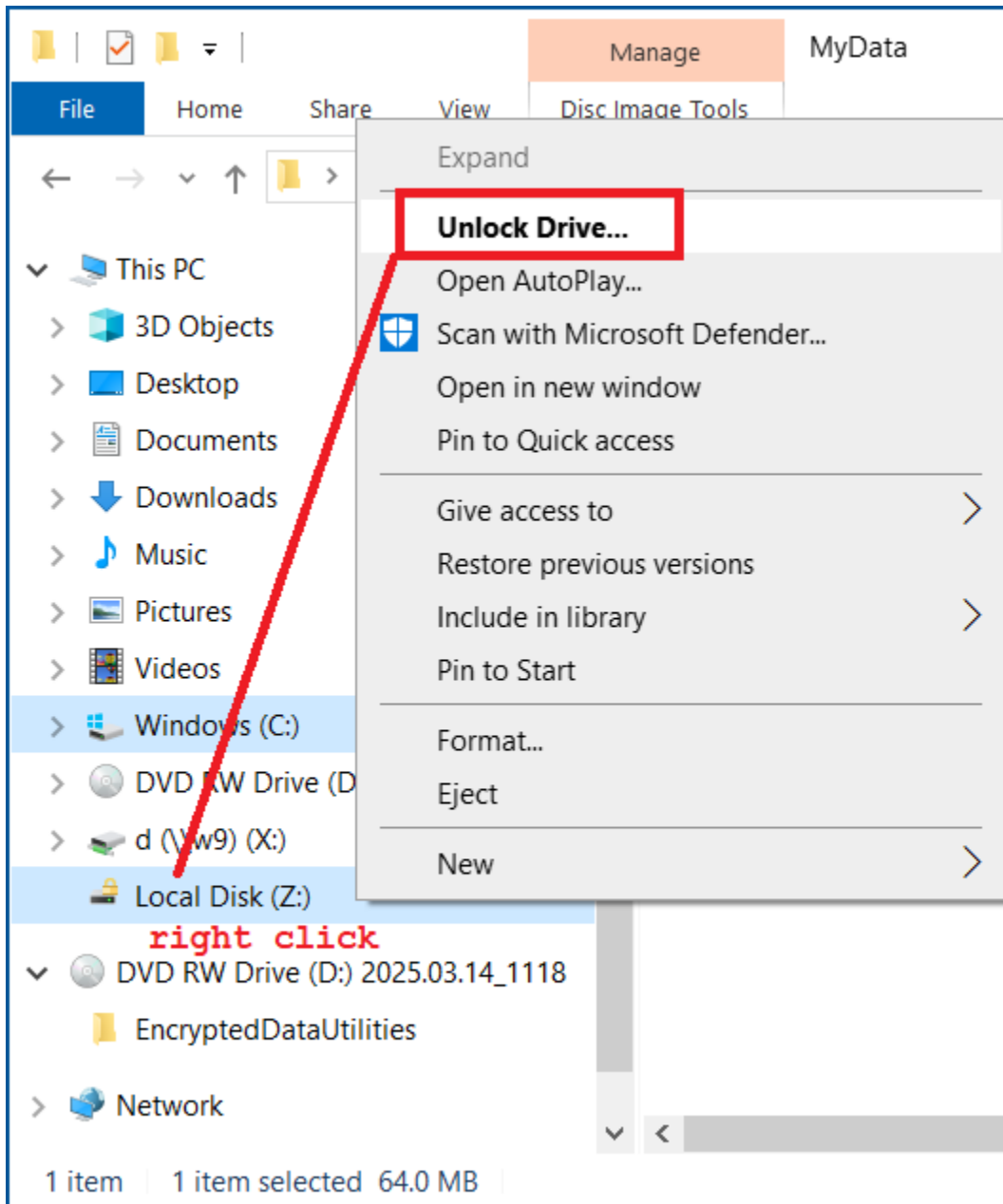


When you click the "Mount", Windows will map a new drive (the Z: drive in the screenshots/example below). The Z: drive needs a password to be able to access it. In the lower right-hand corner of the screen, a pop-up windows will prompt you to "Unlock drive Z:" (it will indicate that "This drive is

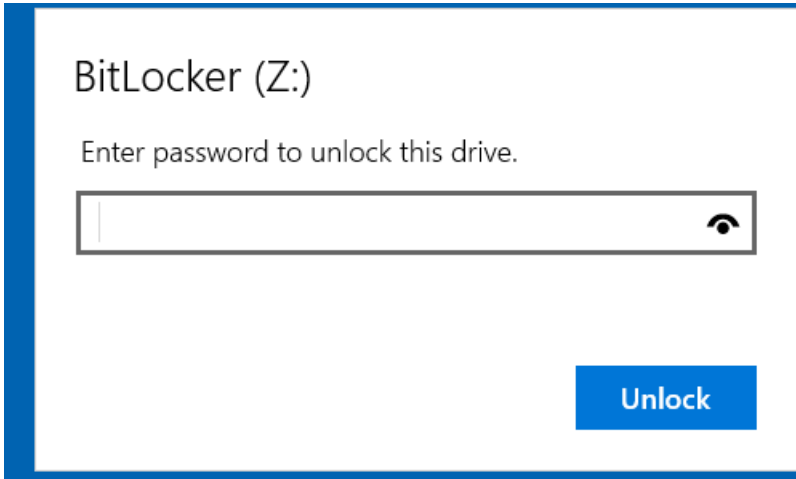
secRMM Administrator Guide

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).

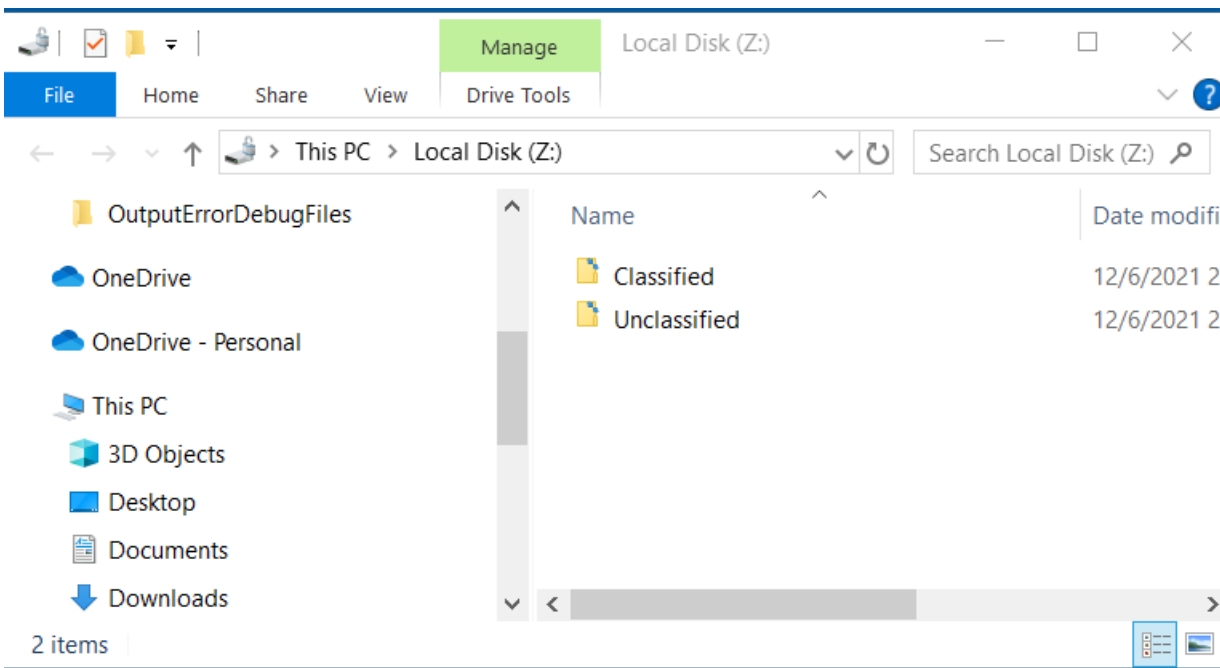




Either way you select to unlock the drive, you will get a window that will prompt you for the password.

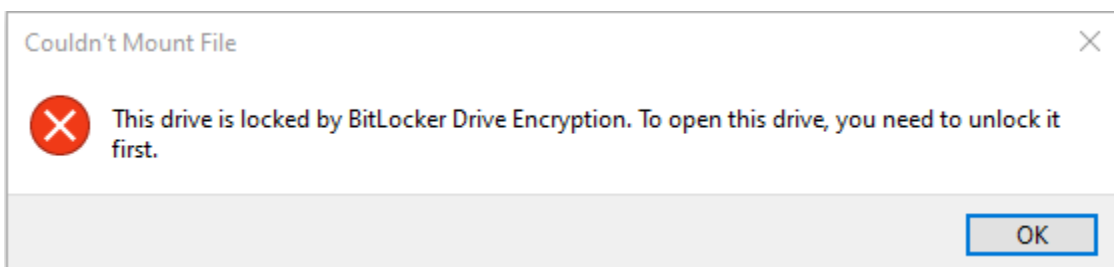


Now specify the password to be able to access the data files.



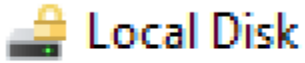
Misleading Windows Explorer pop-up error message

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.



secRMM Encrypted CD/DVD/Blu-ray User Guide

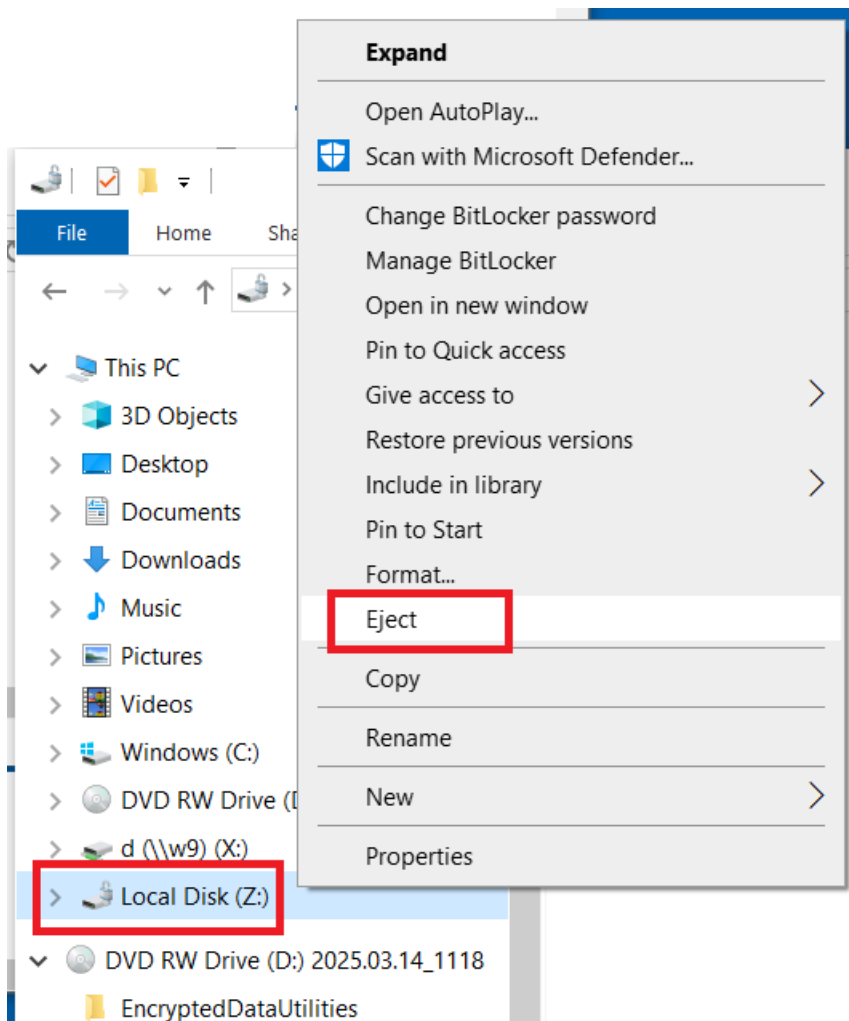
If you see this error, look for a drive with the BitLocker icon as in the screenshot below.



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".



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 support@squadratechnologies.com 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:)
#
*****
```

secRMM Encrypted CD/DVD/Blu-ray User Guide

```
$l_stringNetworkShare = "\\Server\Share"; # change this line for your environment

$l_secureStringPassword = ConvertTo-SecureString -String $stringPassword_in -AsPlainText -Force;

Enable-BitLocker `
-MountPoint $stringVhdDriveLetter_in `
-EncryptionMethod $g_EncryptionStrength `
-UsedSpaceOnly `
-Password $l_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;;

$l_stringRecoveryKey =
(Get-BitLockerVolume -MountPoint $stringVhdDriveLetter_in).KeyProtector `
| Where-Object {$_.KeyProtectorType -eq 'RecoveryPassword'};

$l_stringRecoveryKeyFileName =
("{0}_{1}_{2}_EncryptedCD_BitLocker.txt" -f `
    $env:COMPUTERNAME, `
    $stringVhdDriveLetter_in.Substring(0, 1), `
    $stringCdDriveLetter_in.Substring(0, 1));

if ((Test-Path -Path $l_stringNetworkShare) -eq $true) {
    $l_stringRecoveryKeyCompleteFileName =
        Join-Path -Path $l_stringNetworkShare -ChildPath $l_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
    $l_stringRecoveryKeyCompleteFileName =
        Join-Path -Path $env:TEMP -ChildPath $l_stringRecoveryKeyFileName;
}
```

secRMM Administrator Guide

```
$l_stringRecoveryKey.RecoveryPassword | `
    Out-File -FilePath $l_stringRecoveryKeyCompleteFileName;
```

EncryptCd.ps1 function EncryptVhd uses these 3 variables for status

```
$l_intReturnCode = 0;
$l_stringReturnData = $null;
$l_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

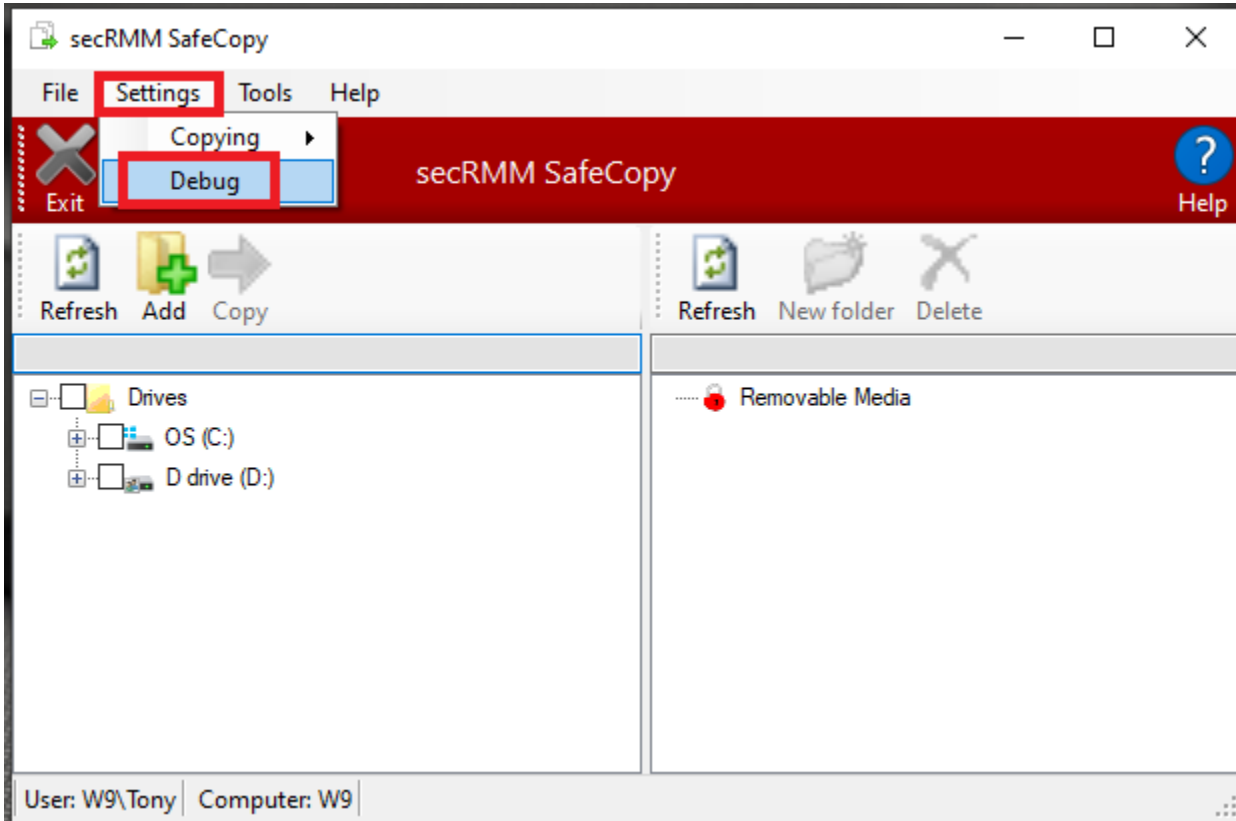
```
.\GetCdInfo.ps1 -stringCdDriveLetter_in e
```

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

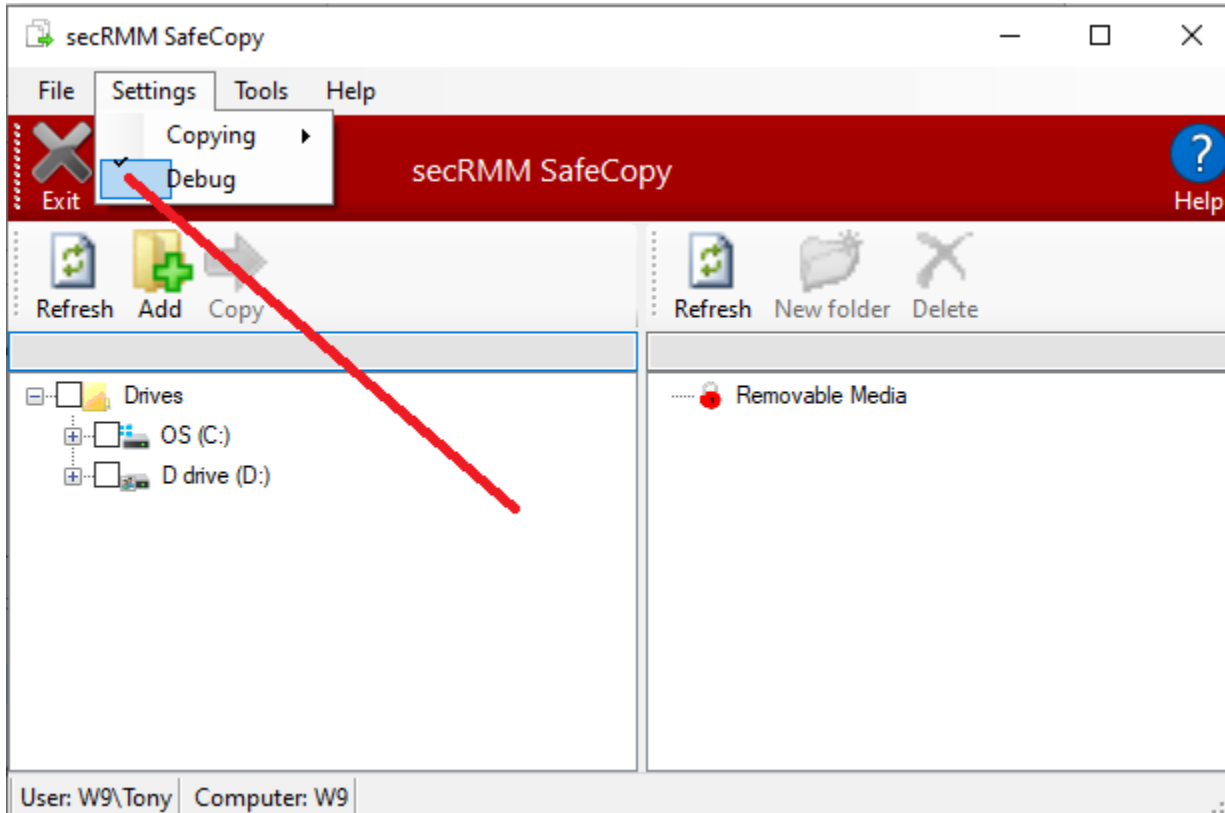
You should encourage your end-users to turn on debugging mode when working with the encrypted discs. In an event where there is an issue, you (and/or Squadra Technologies support) can review the debug logs to identify any issues.

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



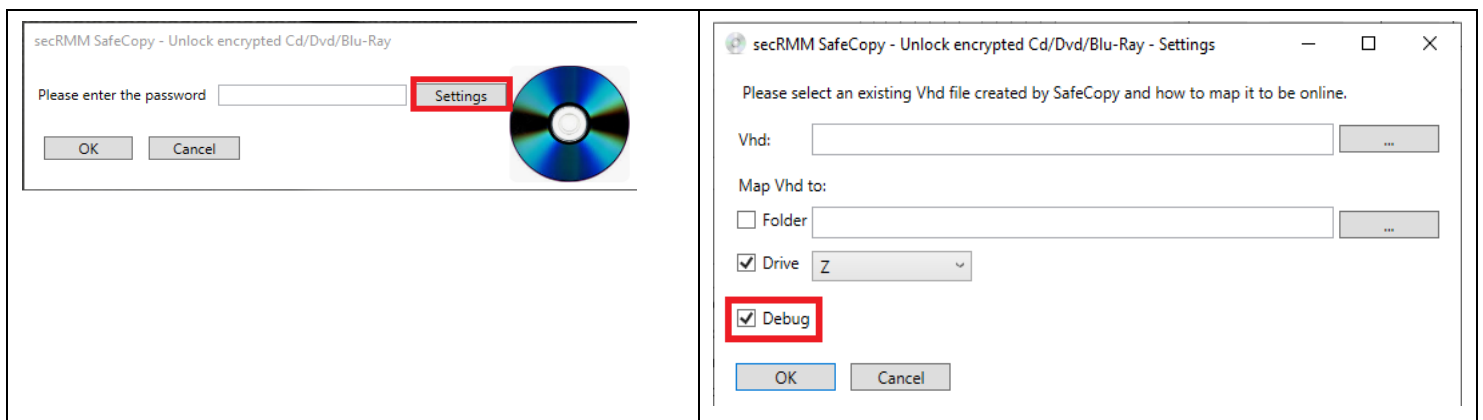
When debugging is turned on, it will look like:

secRMM Administrator Guide

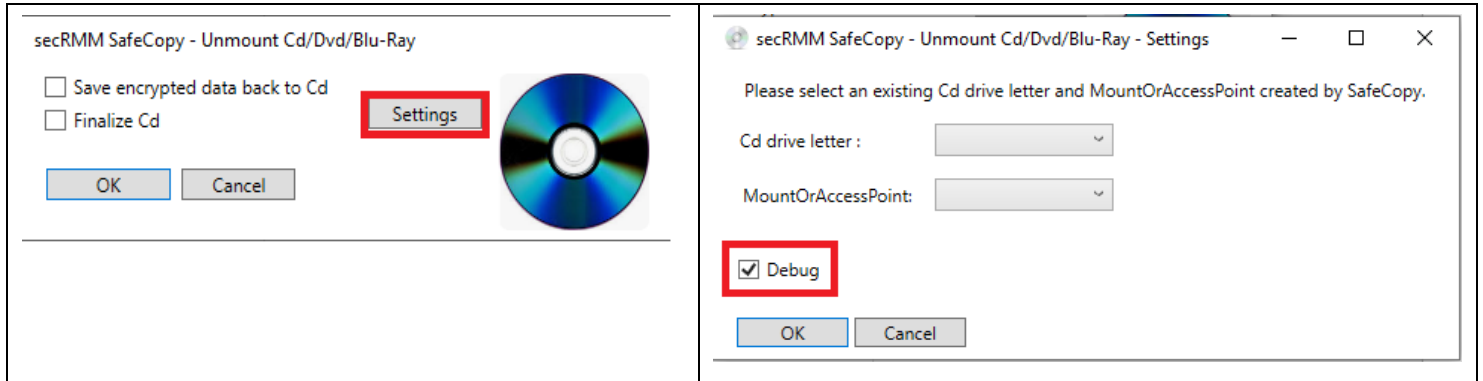


Please note the checkbox indicating that the debugger is turned on is not aligned correctly. This is a Microsoft .Net issue. Once they resolve this issue, we will incorporate it into the secRMMSafeCopy program.

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 Encrypted CD/DVD/Blu-ray User Guide



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

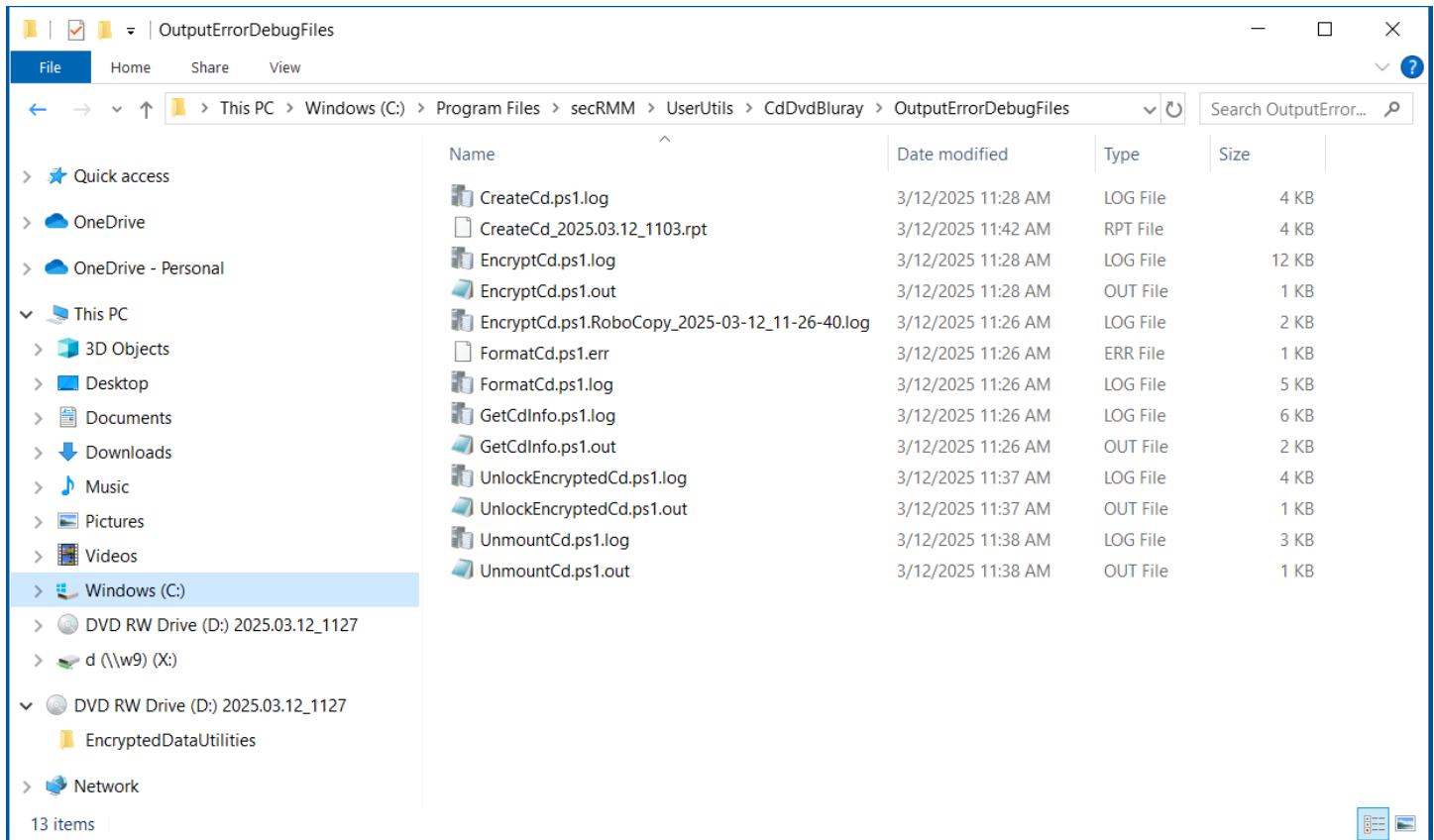
1. `-intDebug_in`
A value of 1 turns debugging on
2. `-stringOutputErrorDebugFilesFolder_in`
Specify an existing directory where you want the debug file(s) (file extension will be .log) to go

```
PS C:\Program Files\secRMM\UserUtils\CdDvdBluray> .\GetCdInfo.ps1 -stringCdDriveLetter_in E: -intDebug_in 1 -stringOutputErrorDebugFilesFolder_in C:\temp
```

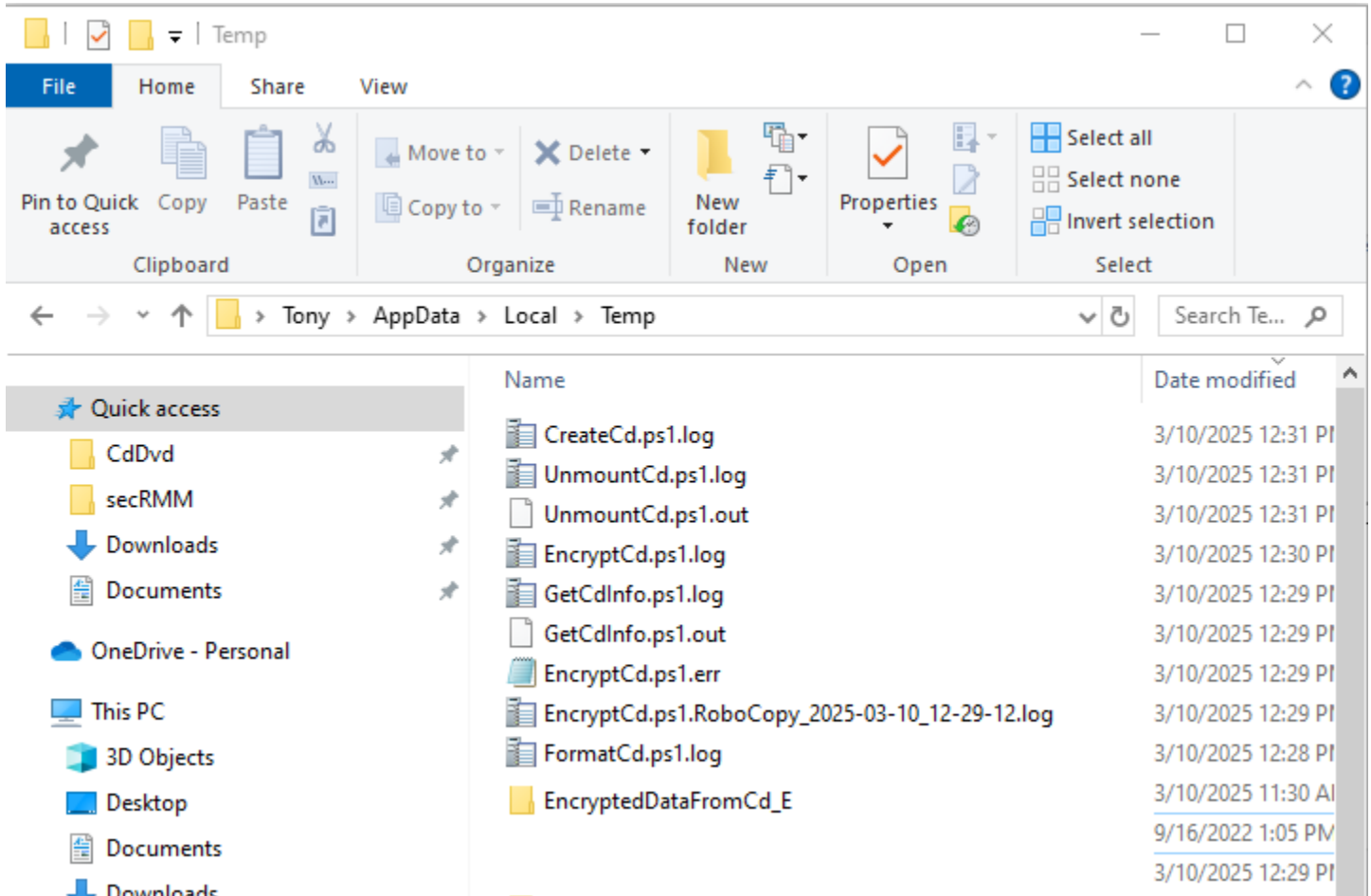
Debug file locations

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



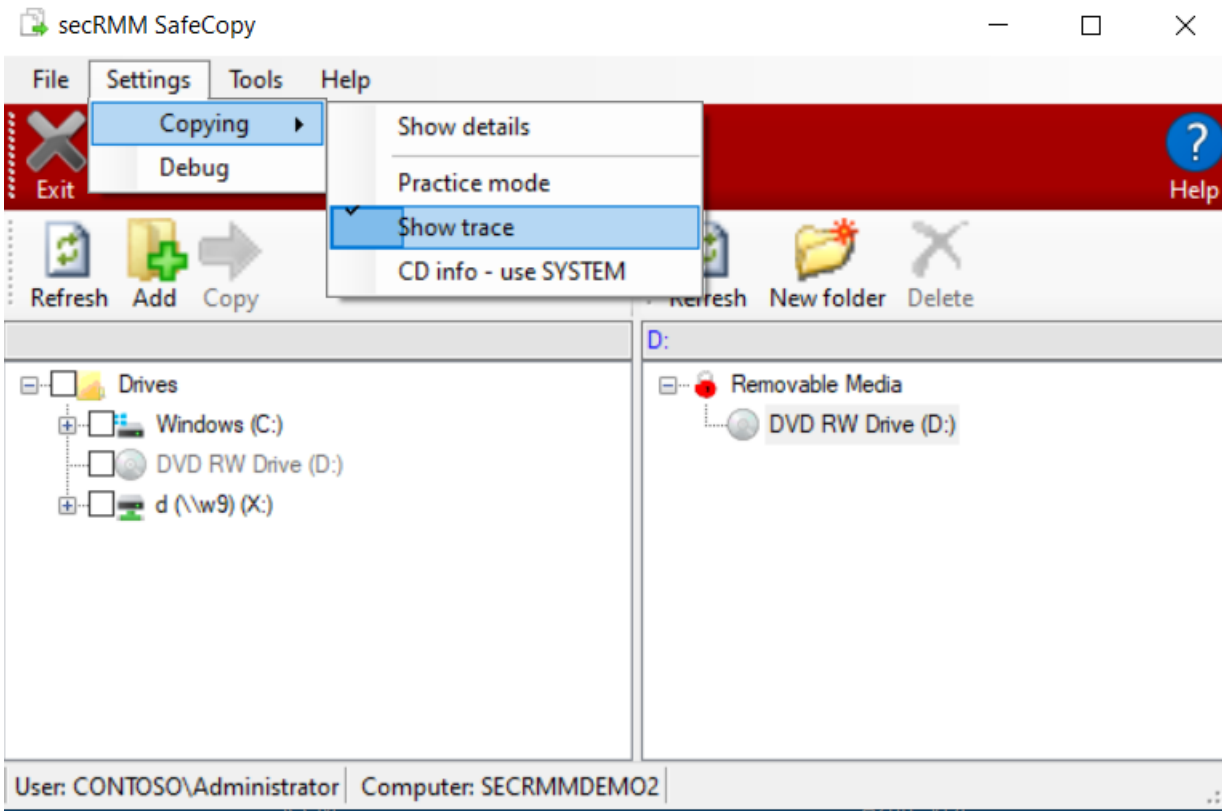
If secRMM is not installed on the computer, the debug files will be located in the users temporary (TEMP environment variable) directory as shown in the screenshot below.

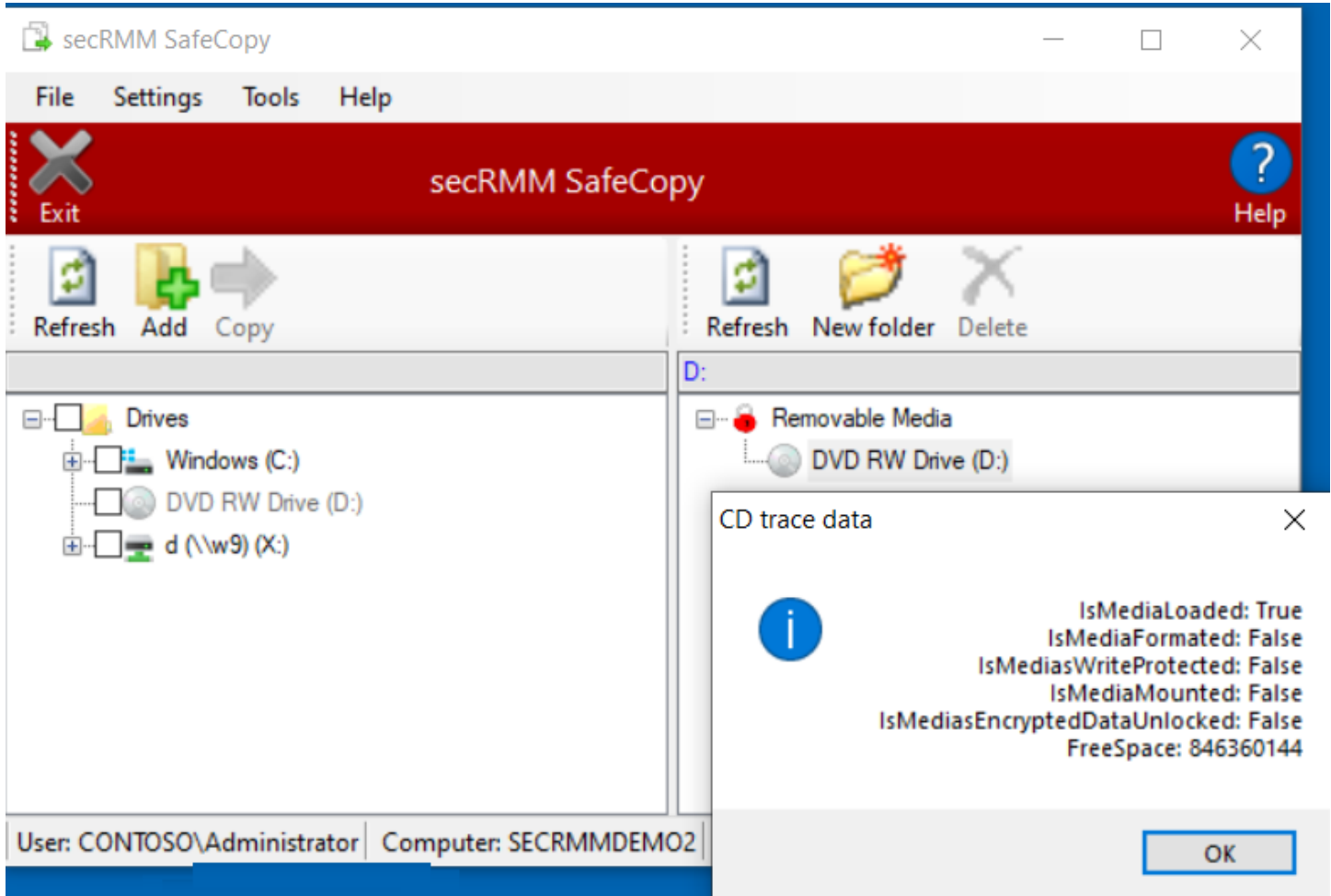


Troubleshooting

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

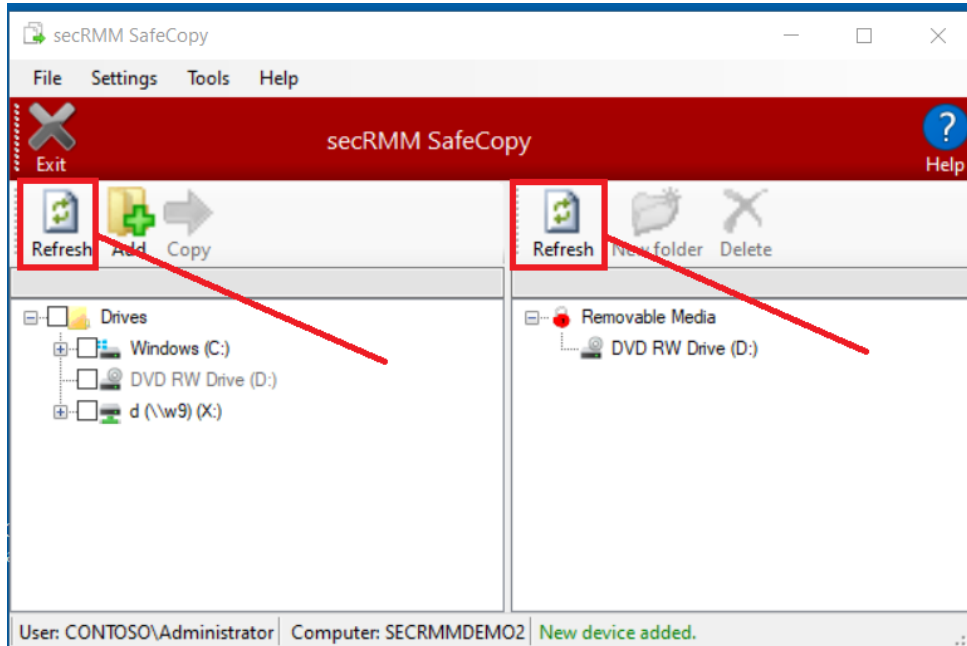




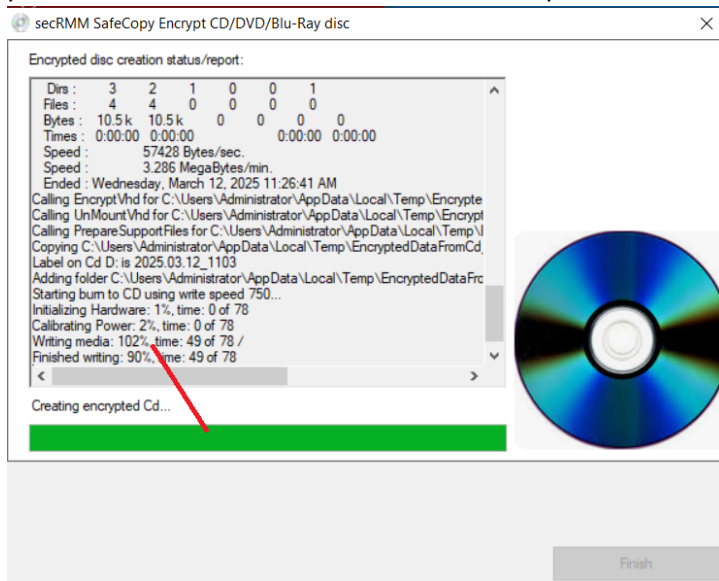
Known issues

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.

secRMM Administrator Guide

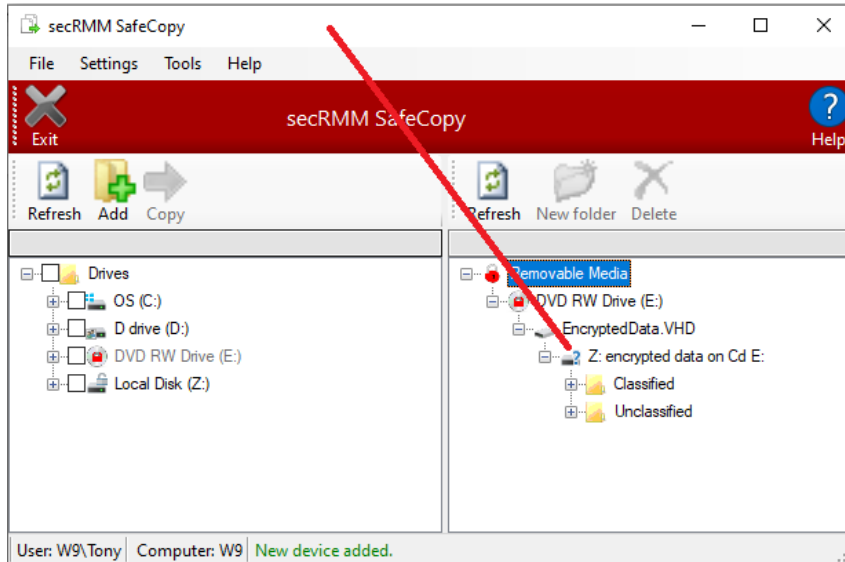


2. When burning a disc, the green progress bar is not able to stay in sync exactly with the burn process. It will look like it is almost complete when there is really more work to be done.

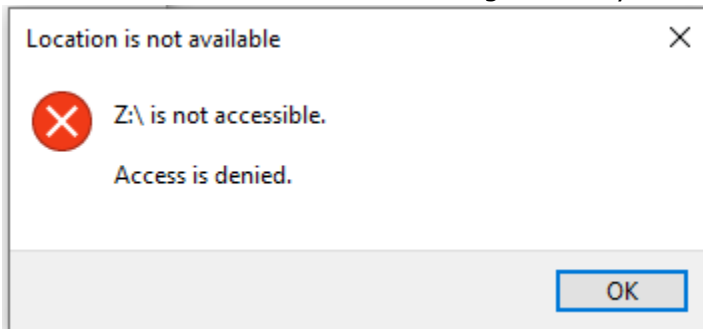


3. The secRMM SafeCopy program shows the BitLocker encrypted container with the wrong icon. We are working on a solution to this issue.

secRMM Encrypted CD/DVD/Blu-ray User Guide

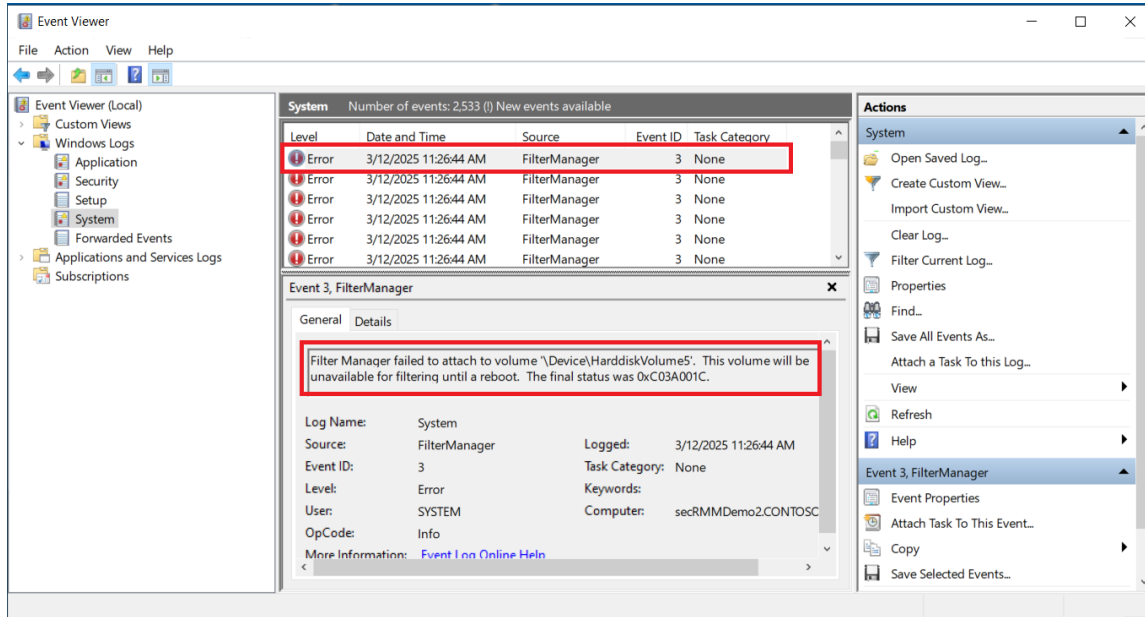


4. When the BitLocker enabled VHD mounts, Windows Explorer sometimes shows a message saying the drive is not accessible. This is a timing issue/bug between BitLocker and Windows Explorer. You can simply click the OK button to dismiss it. We are working on a way to fix this annoying issue/bug.



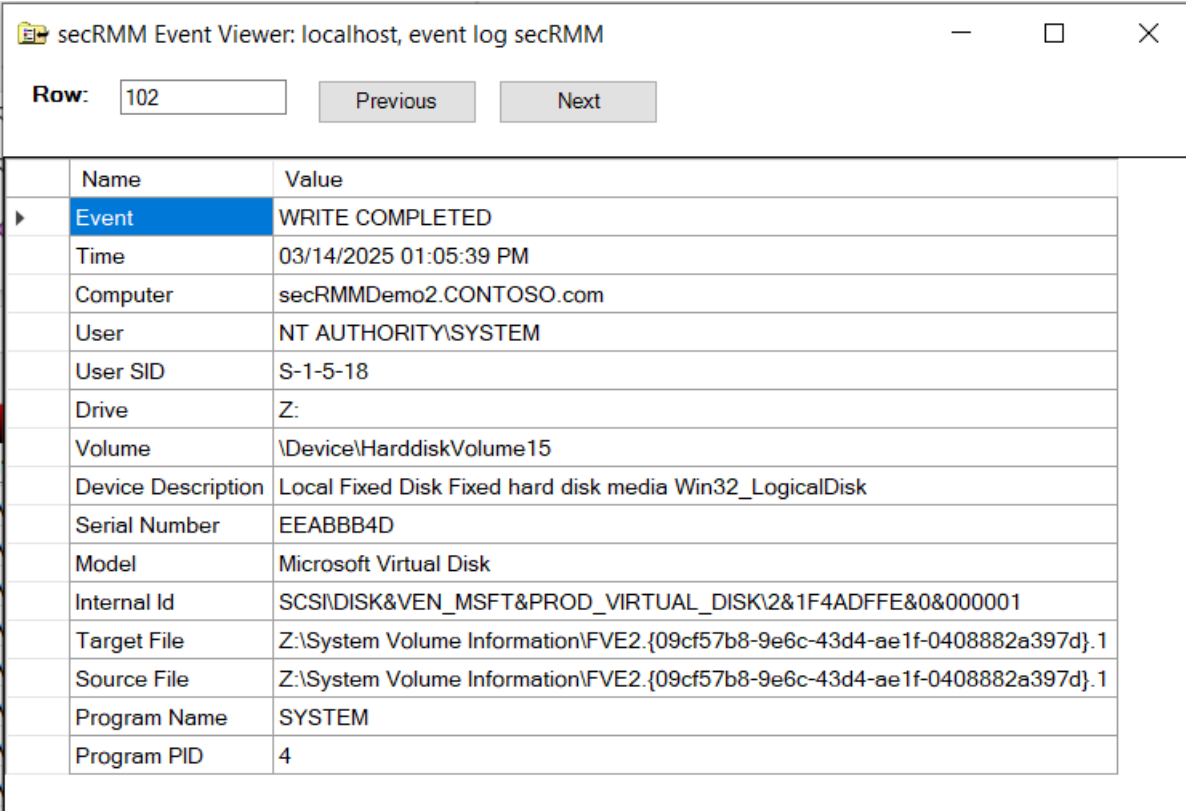
5. When the BitLocker enabled VHD mounts, the Windows System event log gets many error messages where the 'Source' column is 'FilterManager' and the 'Event ID' column is 3. This appears to be related to the 'Windows Search Service'. While annoying, it does not cause any issues. We are working on a way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

secRMM Administrator Guide



- 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.

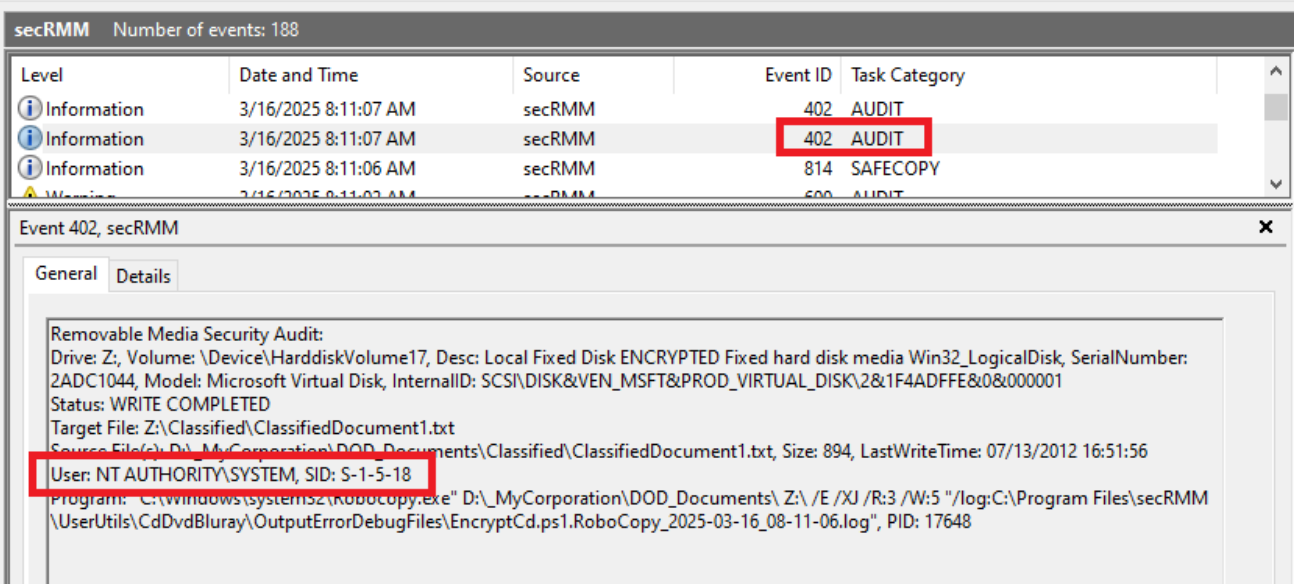
secRMM Encrypted CD/DVD/Blu-ray User Guide



The screenshot shows the 'secRMM Event Viewer' window for 'localhost, event log secRMM'. The 'Row' is set to 102. The event details are as follows:

Name	Value
Event	WRITE COMPLETED
Time	03/14/2025 01:05:39 PM
Computer	secRMMDemo2.CONTOSO.com
User	NT AUTHORITY\SYSTEM
User SID	S-1-5-18
Drive	Z:
Volume	\Device\HarddiskVolume15
Device Description	Local Fixed Disk Fixed hard disk media Win32_LogicalDisk
Serial Number	EEABBB4D
Model	Microsoft Virtual Disk
Internal Id	SCSISDISK&VEN_MSFT&PROD_VIRTUAL_DISK\2&1F4ADFFE&0&000001
Target File	Z:\System Volume Information\FVE2.{09cf57b8-9e6c-43d4-ae1f-0408882a397d}.1
Source File	Z:\System Volume Information\FVE2.{09cf57b8-9e6c-43d4-ae1f-0408882a397d}.1
Program Name	SYSTEM
Program PID	4

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



The screenshot shows the Windows Event Viewer for 'secRMM' with 188 events. Event 402 is highlighted. The details for Event 402 are as follows:

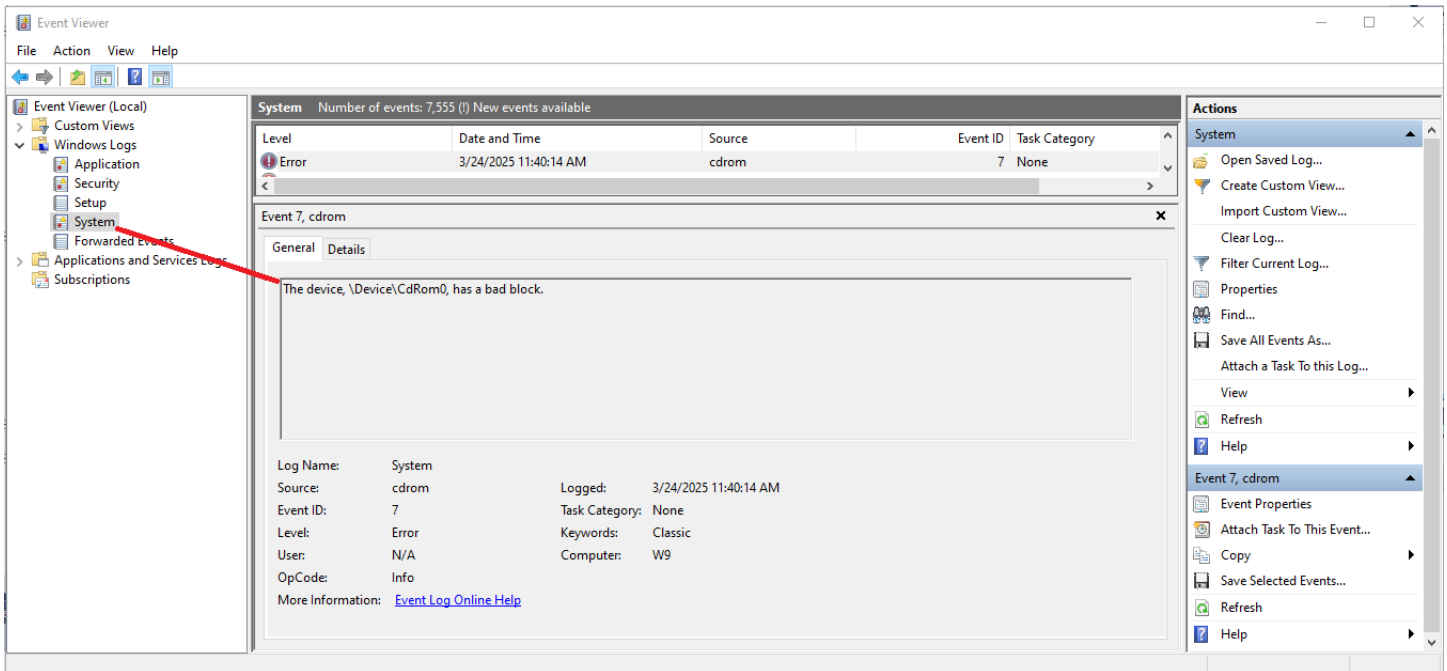
Level	Date and Time	Source	Event ID	Task Category
Information	3/16/2025 8:11:07 AM	secRMM	402	AUDIT
Information	3/16/2025 8:11:07 AM	secRMM	402	AUDIT
Information	3/16/2025 8:11:06 AM	secRMM	814	SAFECOPY
Warning	3/16/2025 8:11:03 AM	secRMM	600	AUDIT

Event 402, secRMM 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&000001
Status: WRITE COMPLETED
Target File: Z:\Classified\ClassifiedDocument1.txt
Source File(s): D:_MyCorporation\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\system32\RoboCopy.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

- Our testing of a Blu-ray drive was not successful. We will work on this issue and post the fix when it becomes available.
- 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.



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.

secRMM Encrypted CD/DVD/Blu-ray User Guide

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/>