squadra technologies

Security Removable Media Manager

connector to

Defender for Cloud

Version 9.11.55.0

(November 2026)

Protect your valuable data

Microsoft Defender for Cloud

© 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, MO 64734
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 Excel AddIn Administrator Guide
Created - August 2011

Contents

INTRODUCTION 4

DESCRIPTION 4
WHY INTEGRATE SECRMM SECURITY EVENTS INTO MICROSOFT DEFENDER FOR CLOUD? 4

CONFIGURATION 5

PREREQUISITES 5
CREATE "AZURE LOG WORKSPACE FOR SECRMM" 5
DOWNLOAD AND IMPORT THE 'SECRMM DEFENDER FOR CLOUD WORKBOOK' 6
CONNECT "AZURE LOG WORKSPACE FOR SECRMM" TO MICROSOFT DEFENDER FOR CLOUD 14
LOADING SECRMM AZURE WORKBOOKS FOR TABULAR REPORTING 15
Prerequisites 16
Azure CLI 16
Download secRMM Azure Workbooks 17
Load secRMM Azure Workbooks using PowerShell 18

USAGE 20

AZURE DEFENDER FOR CLOUD QUERIES 20
Sample query 1 – ONLINE events 20
Sample query 2 – Count the number of failed write attempts events 21
Sample query 3 – Which users are writing files to removable storage devices 22
Sample query 4 – Which users attempted writing files to removable storage devices but failed 22
More sample queries 22
Microsoft BitLocker Activity for removable storage devices 22
Microsoft Windows Defender Activity for removable storage devices 23
Hardware Encrypted Device Activity 24
Users who have tried to execute macros or programs from a removable storage device 24
Removable storage devices that are not encrypted (hardware or software) 25
Removable storage devices that are mounted into a Virtual Machine 26
Event on the physical machine 26
Event on the virtual machine 26
Show mobile devices that are being USB mounted 27
Show mobile devices that are being USB mounted but are not MDM (Microsoft Intune) enrolled 27
AZURE LOG ANALYTICS SECRMM SCHEMA 28
Descriptions 28

CONTACTING SQUADRA TECHNOLOGIES SUPPORT 29

ABOUT SQUADRA TECHNOLOGIES, LLC. 30

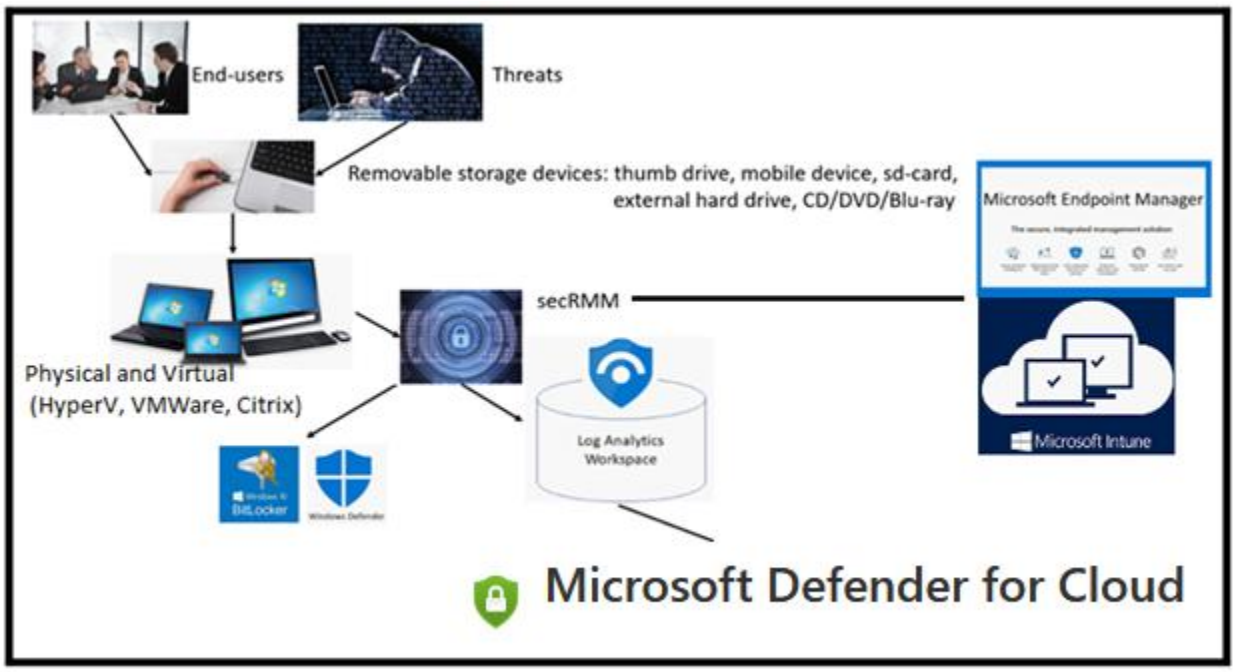
Introduction

Description

Microsoft Defender for Cloud is a Cloud Workload Protection Platform (CWPP) that also delivers Cloud Security Posture Management (CSPM) for all of your Azure, on-premises, and multicloud (Amazon AWS and Google GCP) resources.

secRMM can be configured to send its events to an Azure (Analytics) Log within your company's Azure instance. The Azure Log can then be configured as a data source to your company's Microsoft Defender for Cloud instance. This allows you to see the security events that secRMM generates within Microsoft Defender for Cloud. This architecture is diagramed below. Note that the Windows computers can be either on-premise or in the cloud.

The remainder of this document will use the term "secRMM Connector to Microsoft Defender for Cloud " to refer to this secRMM to Microsoft Defender for Cloud integration.



If you follow the steps in this document, it should take no more than 30 minutes to be up and running.

Why integrate secRMM security events into Microsoft Defender for Cloud?

secRMM is a Windows security solution that monitors/audits and protects (via policies) all removable storage within your on-premise and cloud environments.

In this context, removable storage 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.

If you plan to use Microsoft Defender for Cloud as one of your centralized security tools, it is only logical that you incorporate the very important security events around removable storage. Removable storage, while very convenient for workers, is a major cause of "Data Loss Prevention" (DLP)/"Insider Threat Protection" (ITP) incidents and introductions of malware into a computing environment.

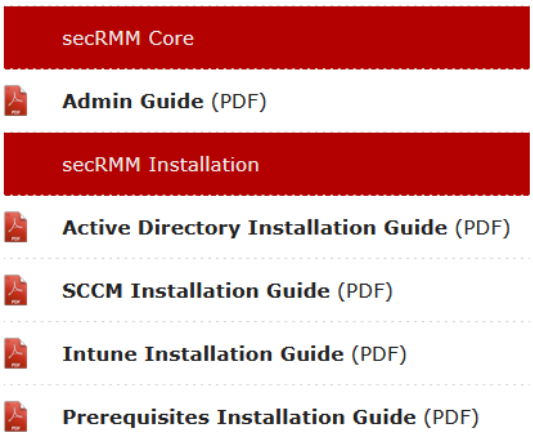
Configuration

Prerequisites

To use the "secRMM Connector to Microsoft Defender for Cloud ", you must first have:

1. An Azure instance (i.e. tenant) for your organization
2. A secRMM deployment which can be for both your physical and virtual Windows computers.

   Deploying secRMM can occur using Active Directory, System Center Configuration Manager (SCCM), Intune or any other Windows software deployment tool. A secRMM deployment is a standard Windows MSI file installation. The documentation to deploy secRMM is on the Squadra Technologies web site at: http://www.squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx, under the "secRMM Installation" section (as shown in the screenshot below).

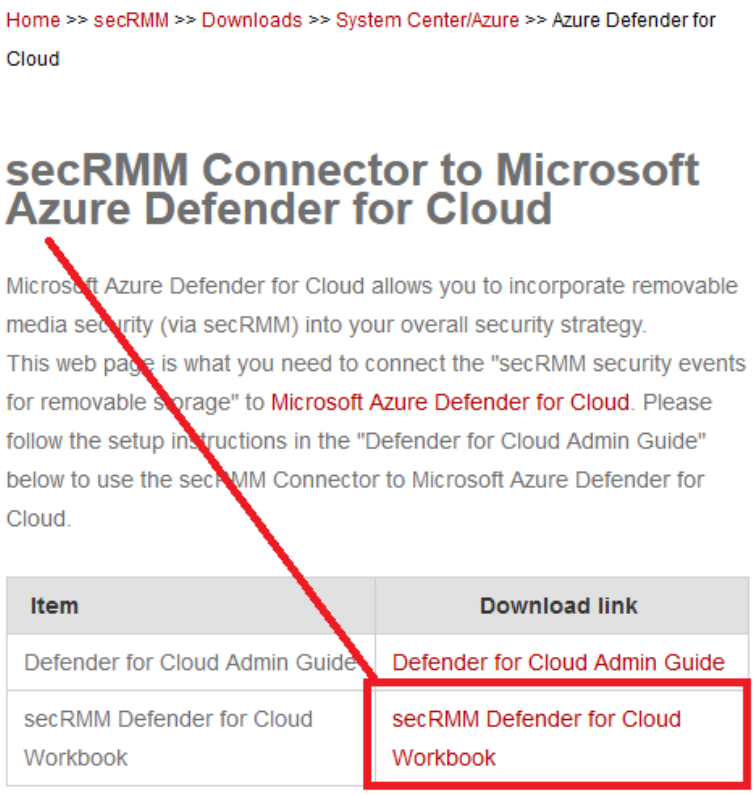


Create "Azure Log Workspace for secRMM"

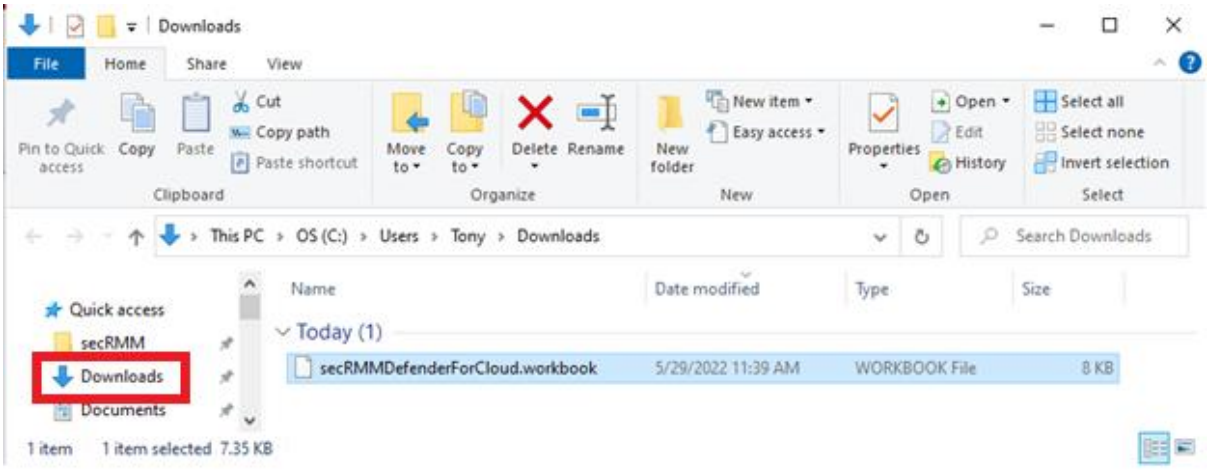
Please follow the **secRMM "Azure Log Analytics Administrator Guide"** to setup your Azure tenant. This documentation is separate from this document because the secRMM Azure Log Analytics Workspace is a common dataset for all of the Azure integrations.

Download and import the 'secRMM Defender for Cloud Workbook'

You download the 'secRMM Defender for Cloud Workbook' from the Squadra technologies web site at: secRMM Azure Defender For Cloud by clicking the 'secRMM Defender for Cloud Workbook' link as shown in the screenshot below.

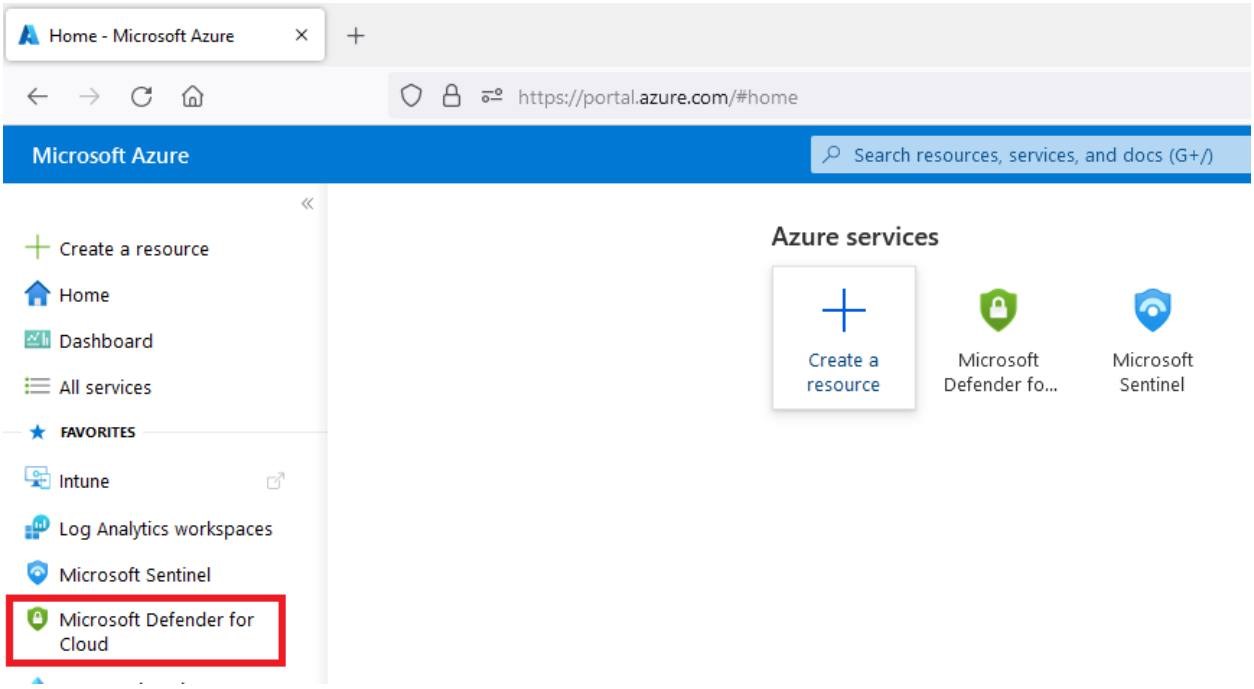


Clicking the 'secRMM Defender for Cloud Workbook' link will download the workbook to your downloads folder as shown in the screenshot below.

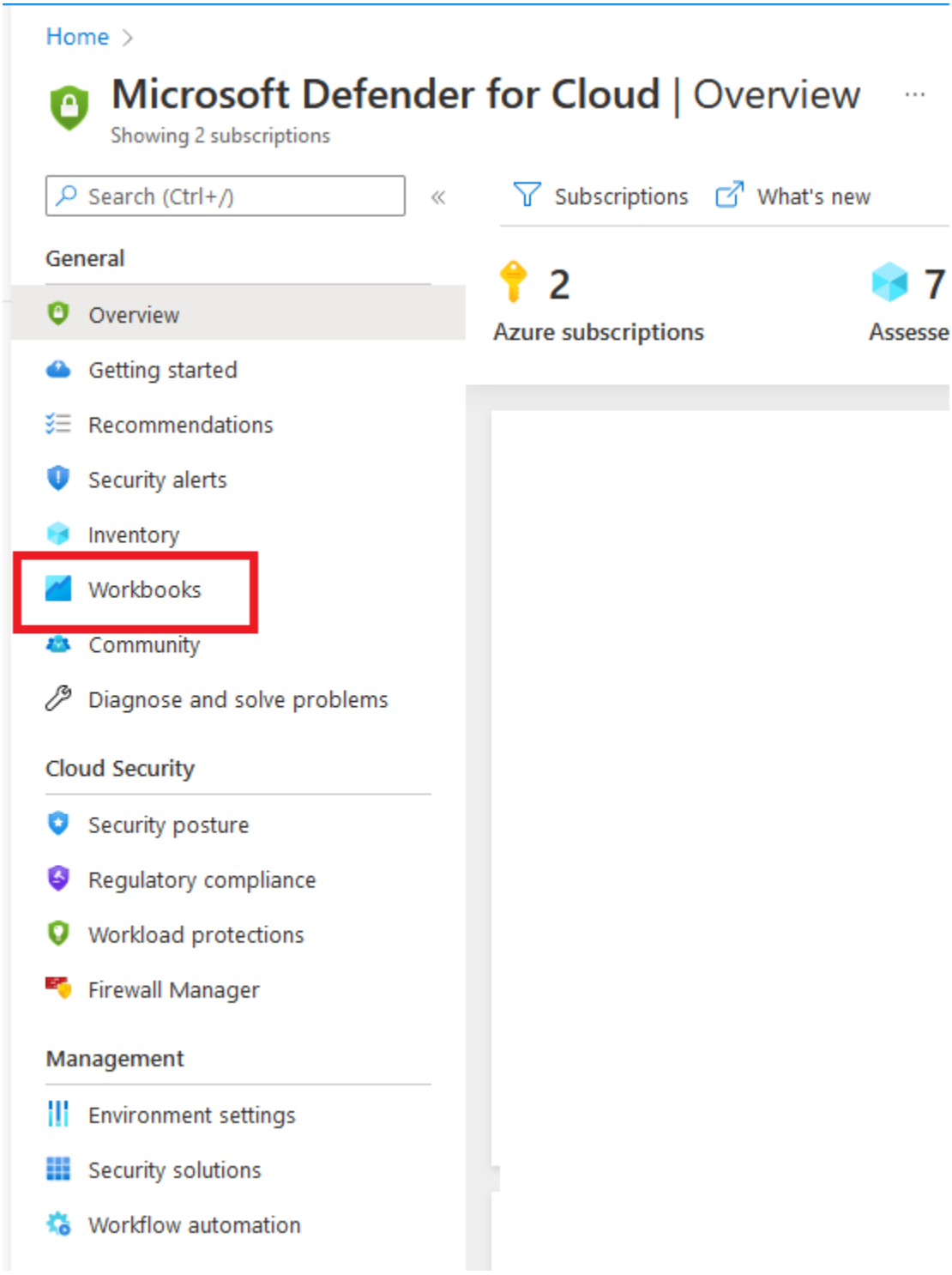


The next few steps will take the 'secRMM Defender for Cloud Workbook' (i.e. the file secRMMDefenderForCloud.workbook you just downloaded) and import (load) it into your Defender for Cloud instance within your Azure tenant. There currently is no nice import function for this but hopefully, eventually, Microsoft will create one.

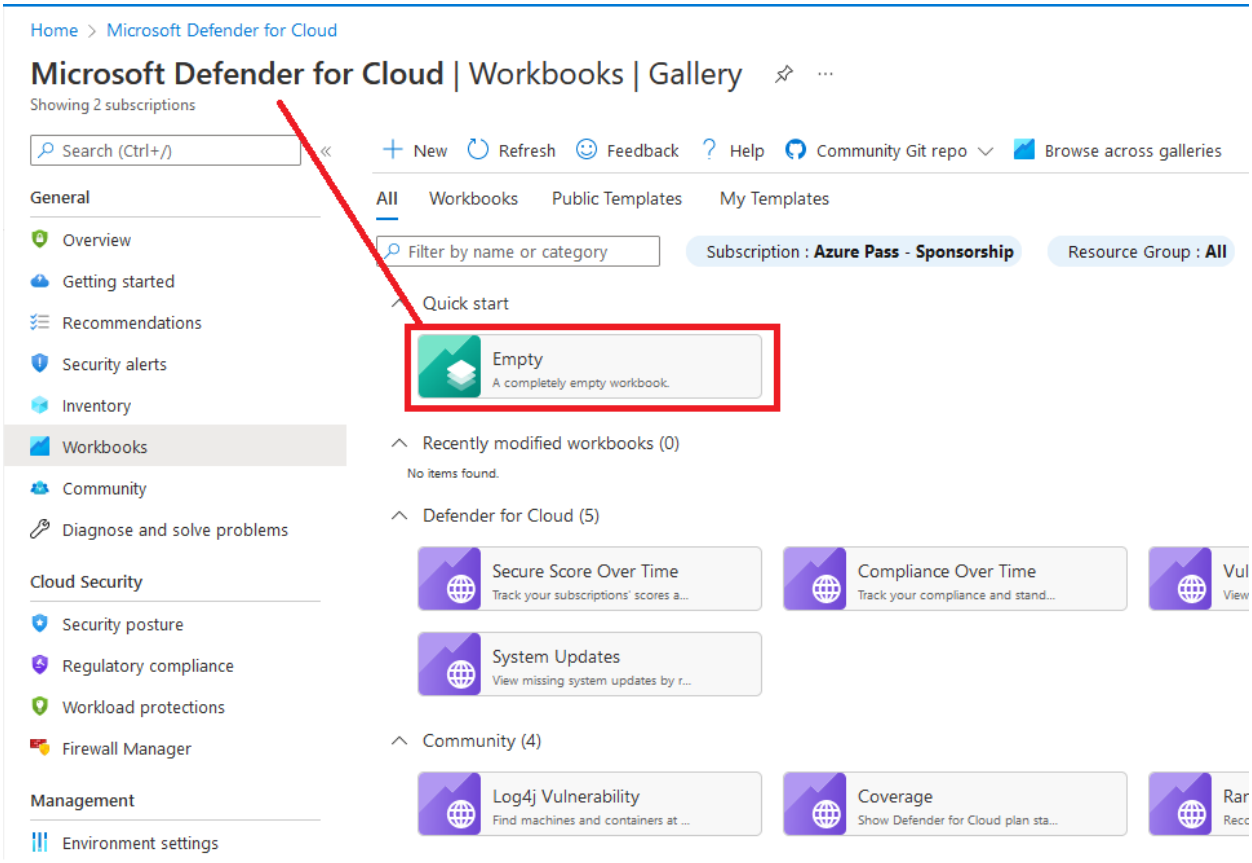
Go to your Azure portal and select your 'Defender for Cloud' instance as shown in the screenshot below. If you do not see 'Microsoft Defender for Cloud' in your Azure portal home page, you can do a search for it using the 'Search resources, services and docs' feature.



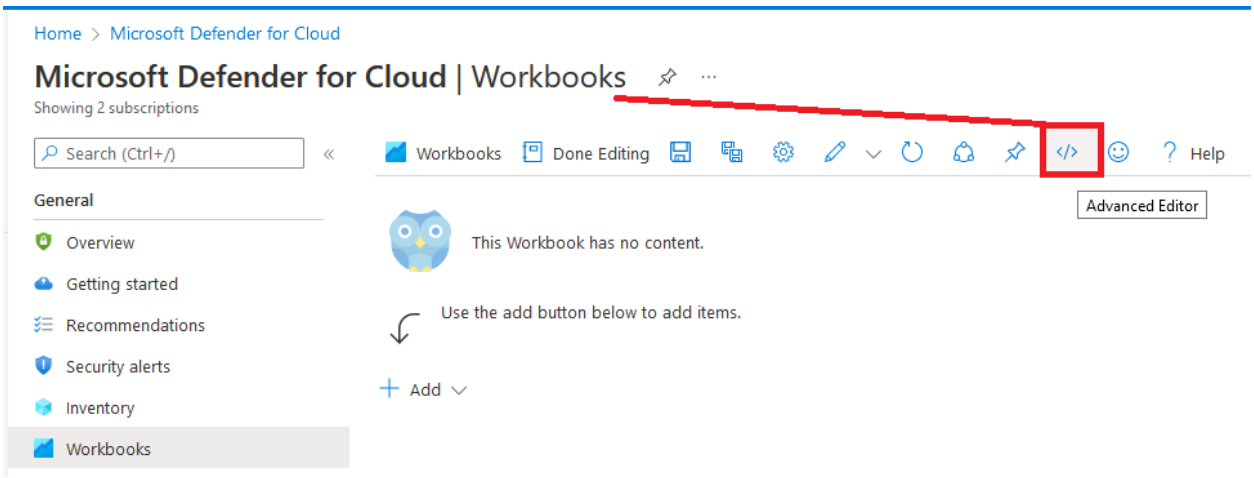
On the 'Microsoft Defender for Cloud' page, click 'Workbooks' as shown in the screenshot below.



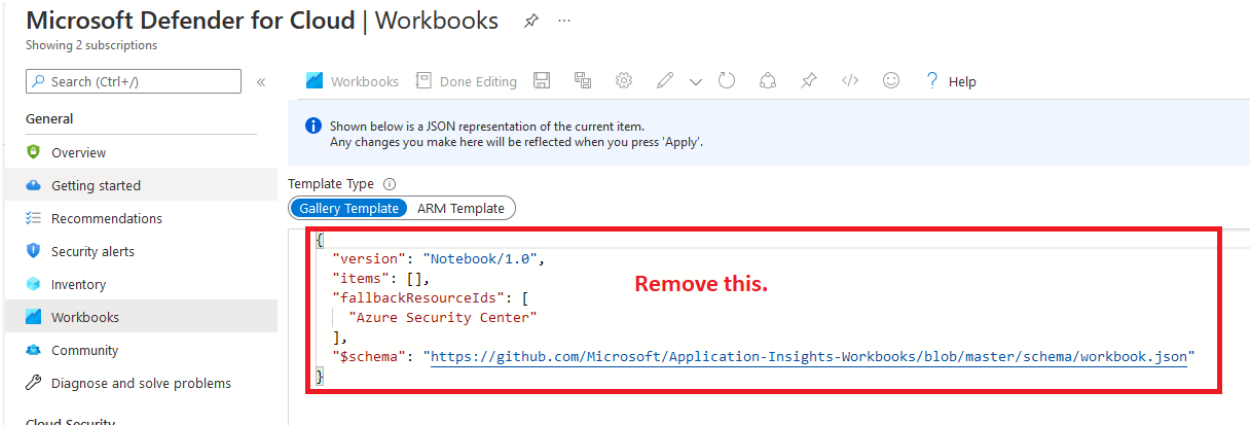
On the 'Microsoft Defender for Cloud Workbooks' page, click the 'Empty' workbook as shown in the screenshot below.



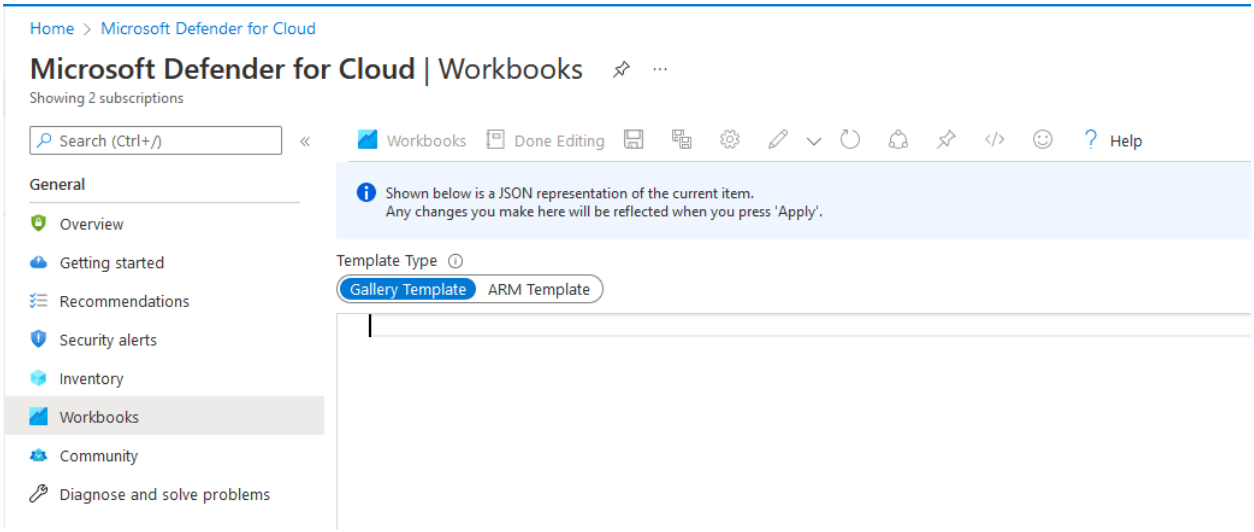
On the page, click the 'Advanced Editor' link as shown in the screenshot below.



On the page, remove the existing json from the editor as shown in the screenshot below.

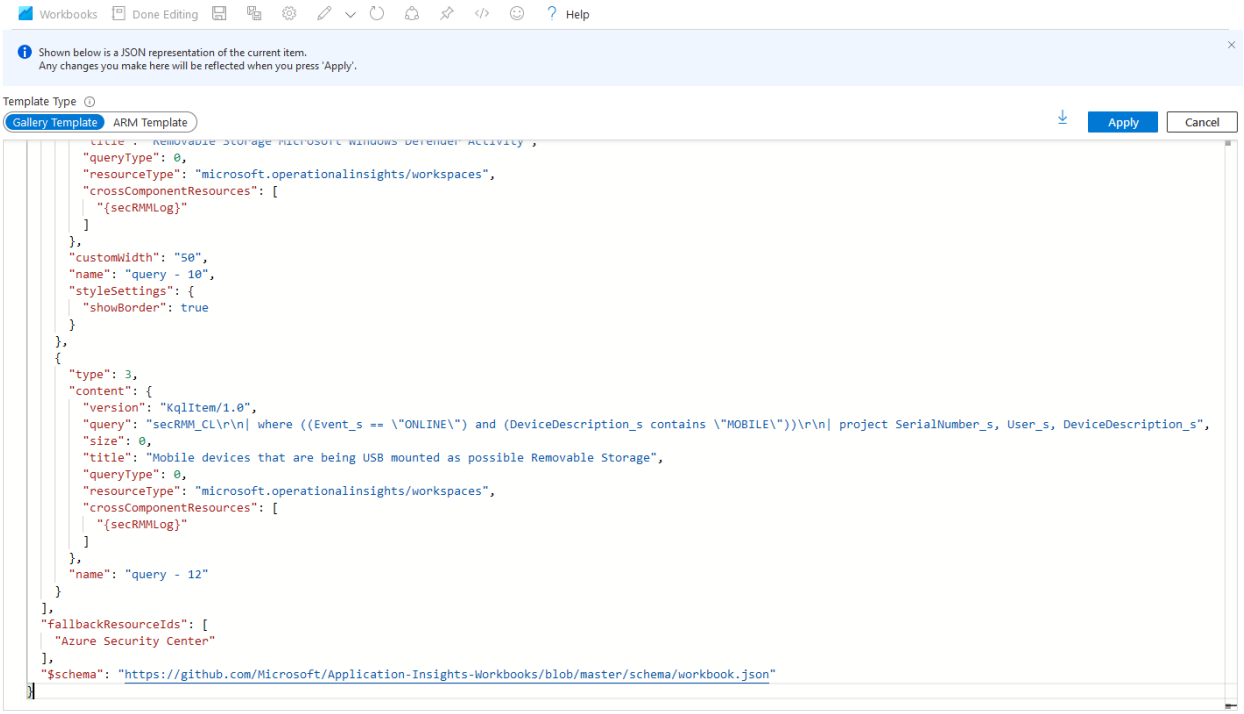


The page will now look like the screenshot below.

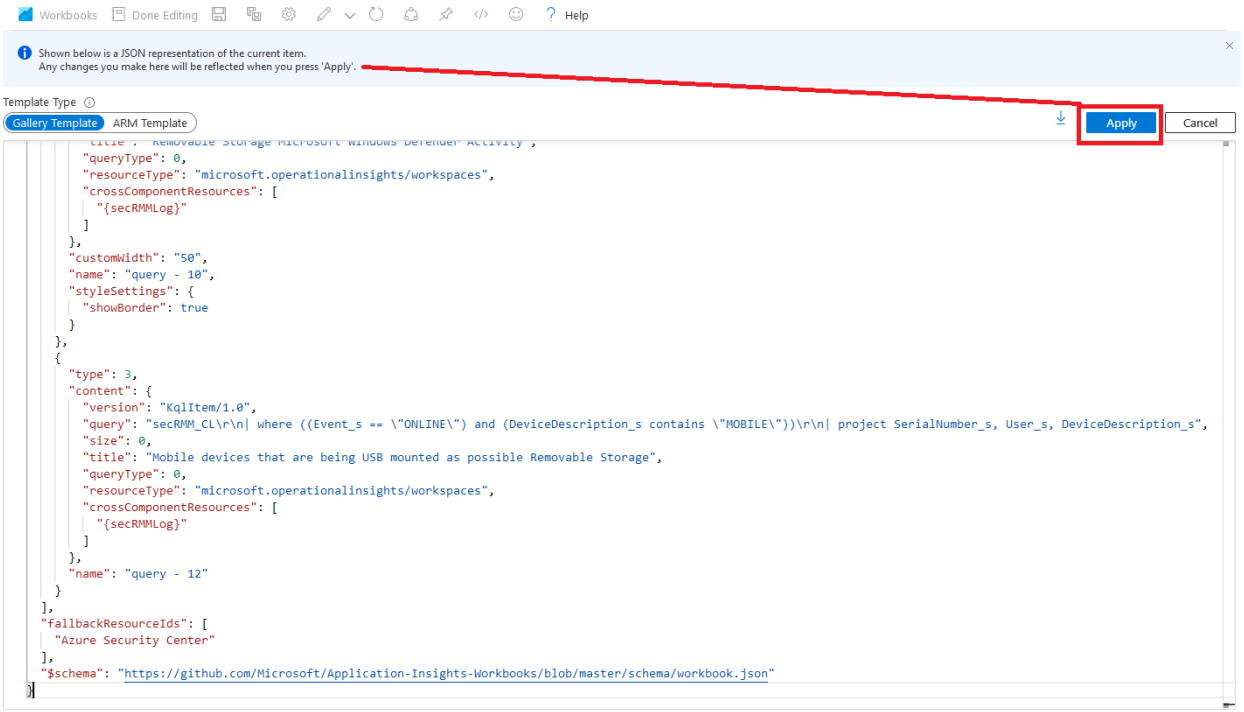


Now, copy (you can just use notepad to open and copy the lines) all the lines in the file named secRMMDefenderForCloud.workbook (which is in your downloads folder from above) and paste all the lines into the page (where you just cleared out all the json.

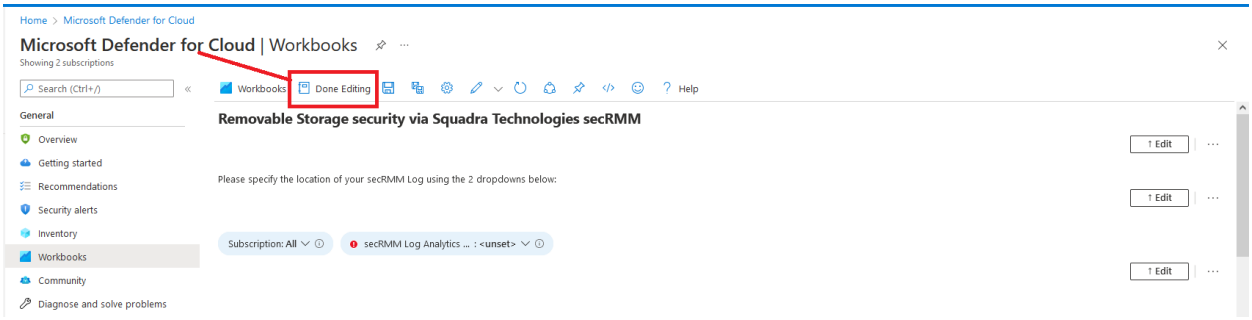
The page will now look like the screenshot below.



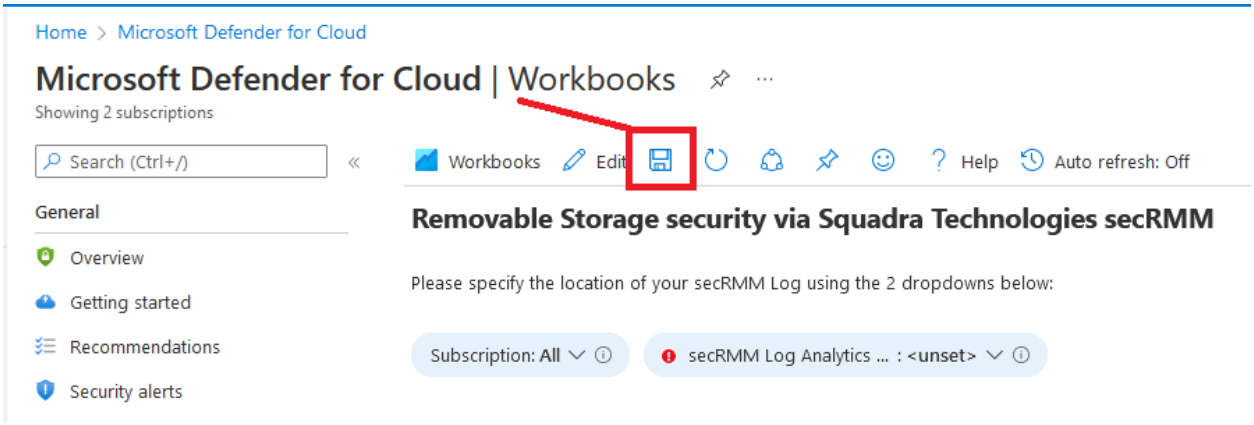
Click the 'Apply' button as shown in the screenshot below.



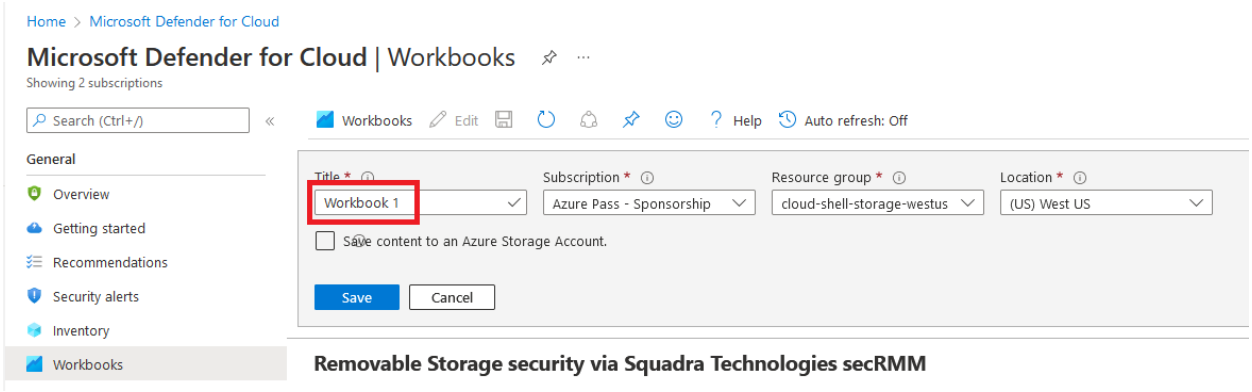
Now click the 'Done Editing' button as shown in the screenshot below.

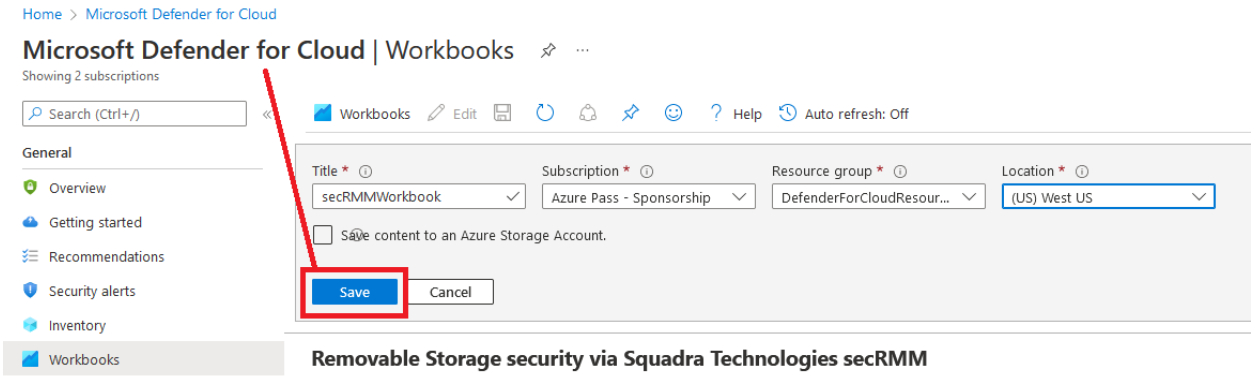


Now click the 'Save' button as shown in the screenshot below.



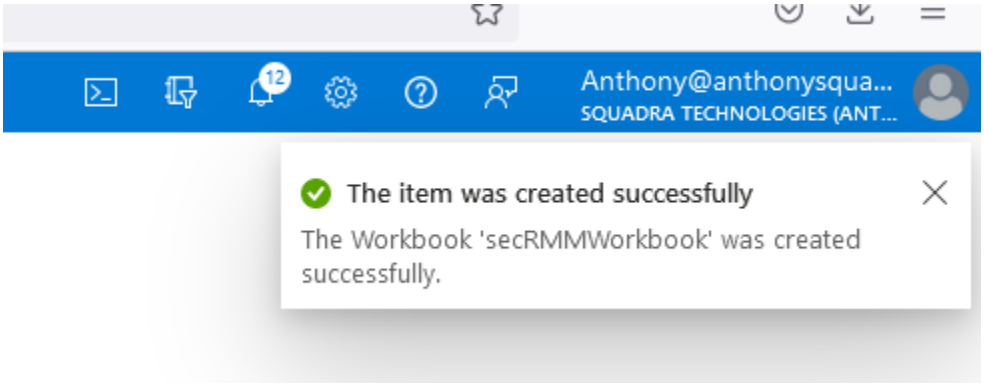
You can name the workbook anything you like.
We suggest naming the secRMMWorkbook.
You can also modify the Subscription and/or Resource group and/or Location values to match your Azure tenant.
Then, click the 'Save' button as shown in the second screenshot below.



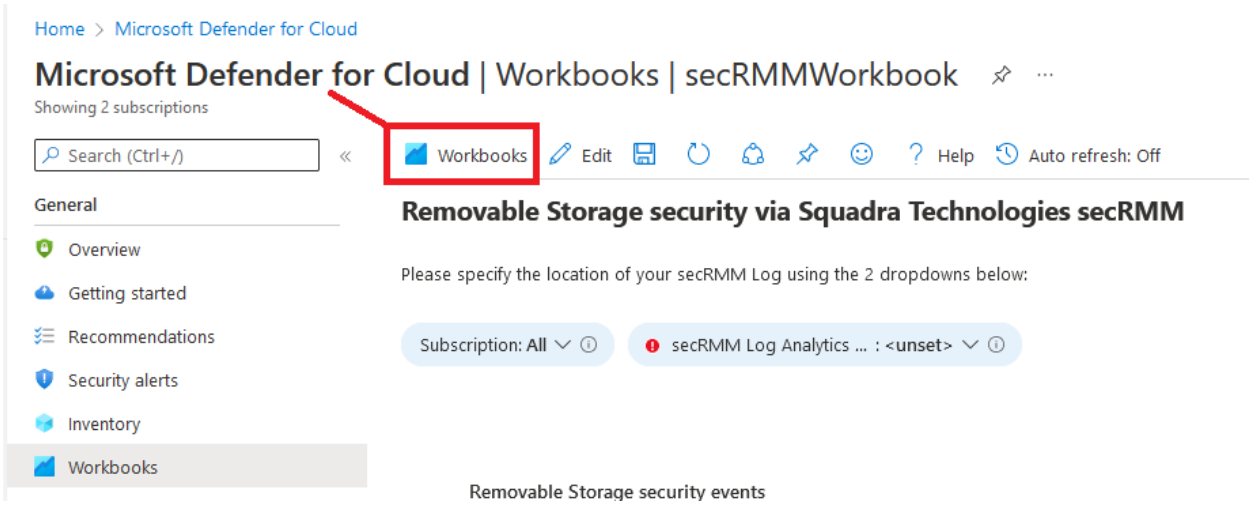


Removable Storage security via Squadra Technologies secRMM

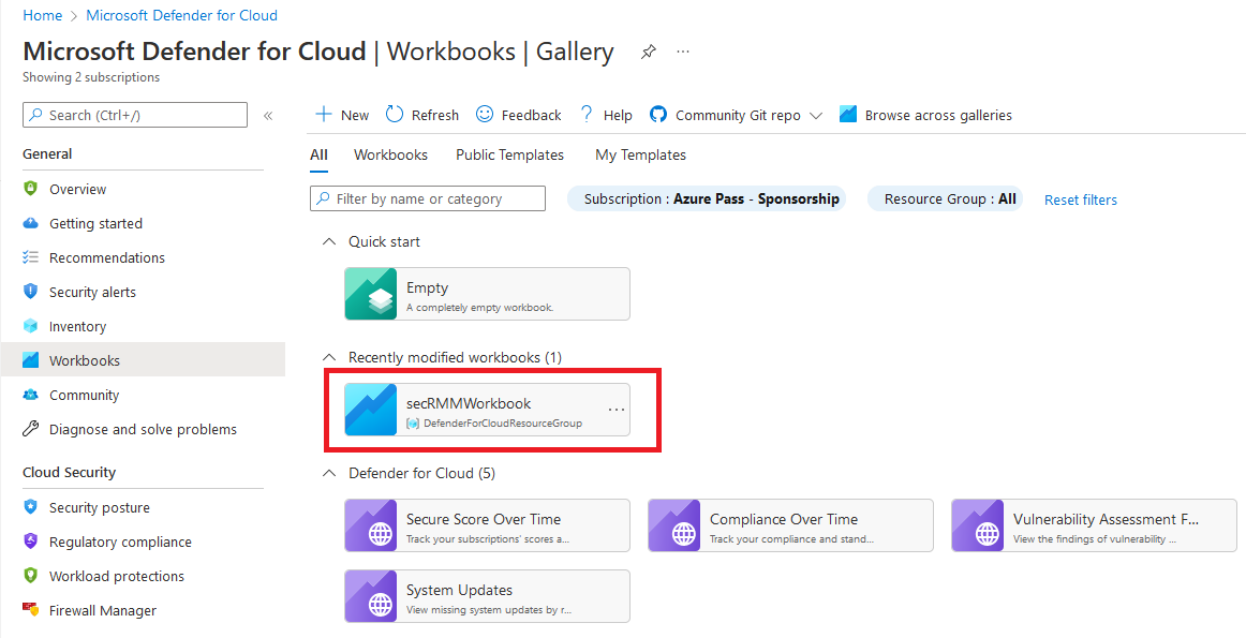
Azure will save the workbook and you will get a notification as shown in the screenshot below.



Now, if you click the workbooks button as shown in the screenshot below.



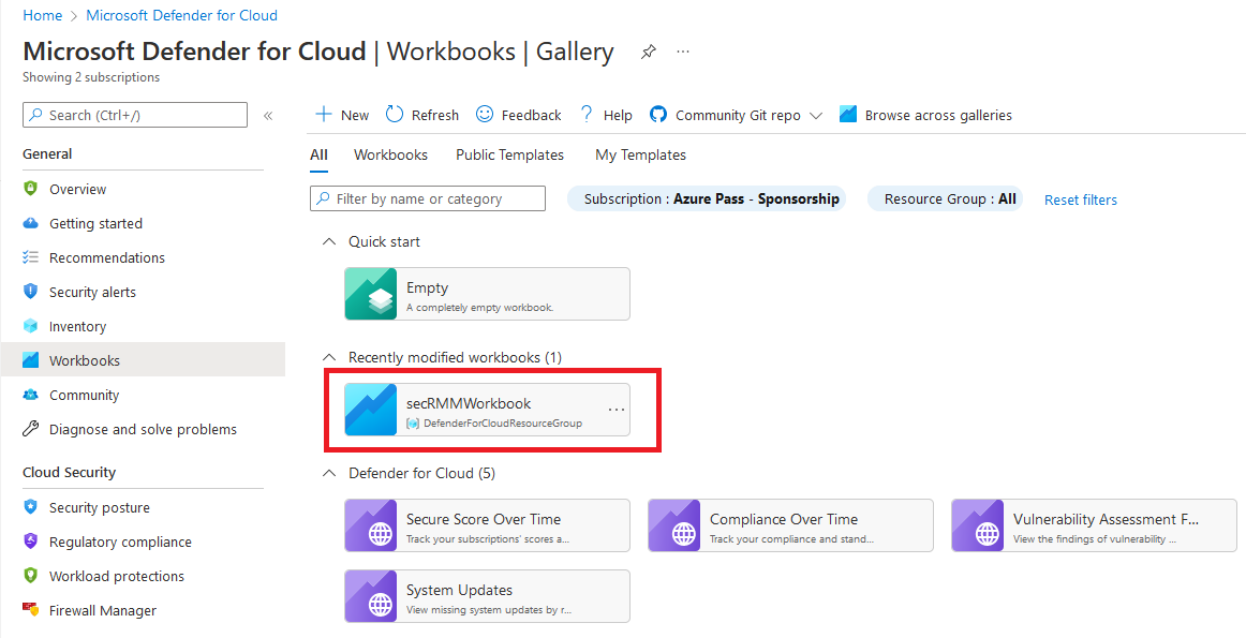
You will now see the secRMMWorkbook in the collection of 'Defender for Cloud' workbooks as shown in the screenshot below.



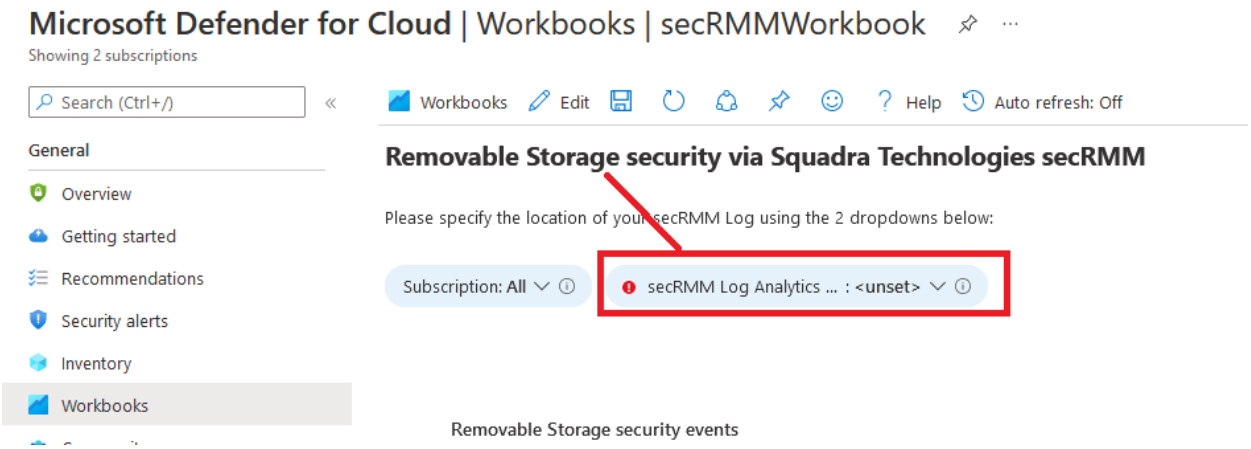
Connect "Azure Log Workspace for secRMM" to Microsoft Defender for Cloud

Now that you have created an "Azure Log Workspace for secRMM" (from the subsection above) and you have downloaded and imported the "secRMM Defender for Cloud workbook", you can connect the "Azure Log Workspace for secRMM" to your "Defender for Cloud workbook for secRMM".

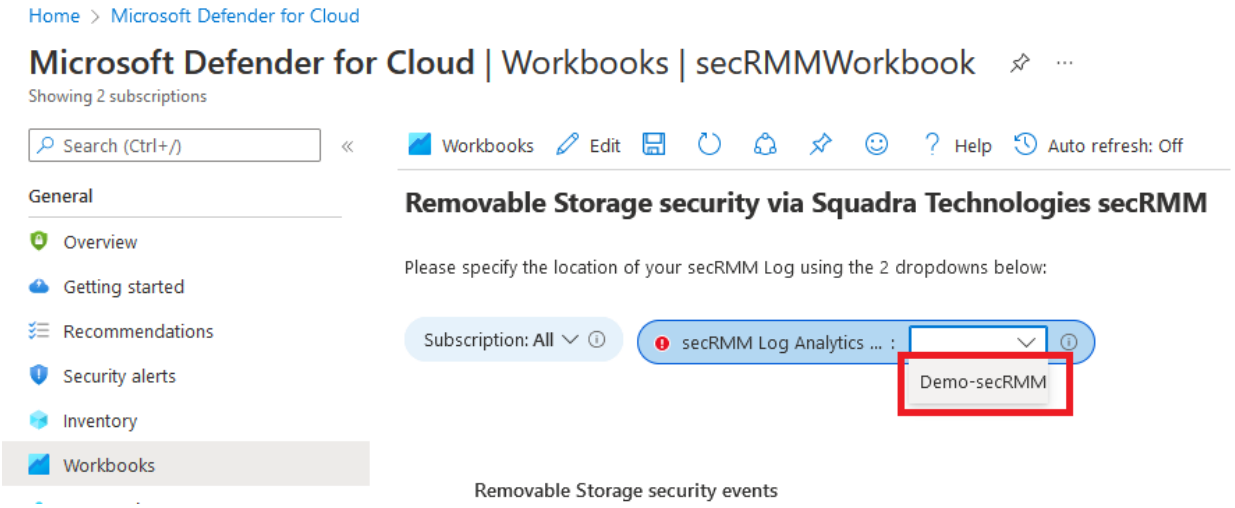
Click the "secRMM Defender for Cloud workbook" you just created as shown in the screenshot below.



Click the 'secRMM Log Analytics' drop-down as shown in the screenshot below.



In the drop-down list, you will see the 'Azure Log Workspace for secRMM' as shown in the screenshot below (note that the name of your workspace will be different from the name in the screenshot below).



Once you select the workspace, the workbook will be ready to render the security events generated by secRMM. The next section shows how to tell secRMM to send the security events to the 'Azure Log Workspace'.

Loading secRMM Azure Workbooks for tabular reporting

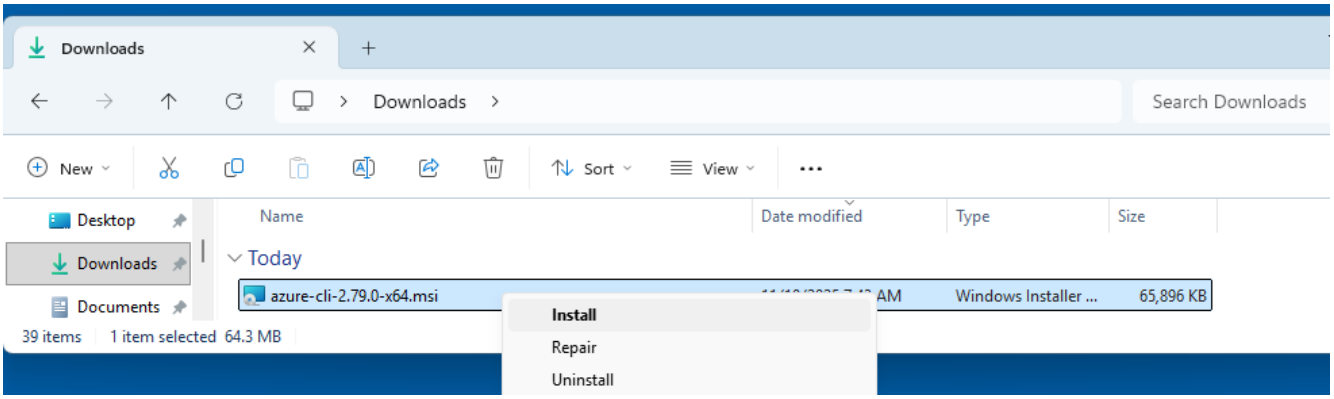
secRMM provides Azure Workbooks (reports) you can run to view the details of the secRMM data.

Prerequisites

Azure CLI

Loading the ‘secRMM Azure Workbooks’ into your Azure tenant requires that the 'Azure CLI' is installed and at version 2.x.

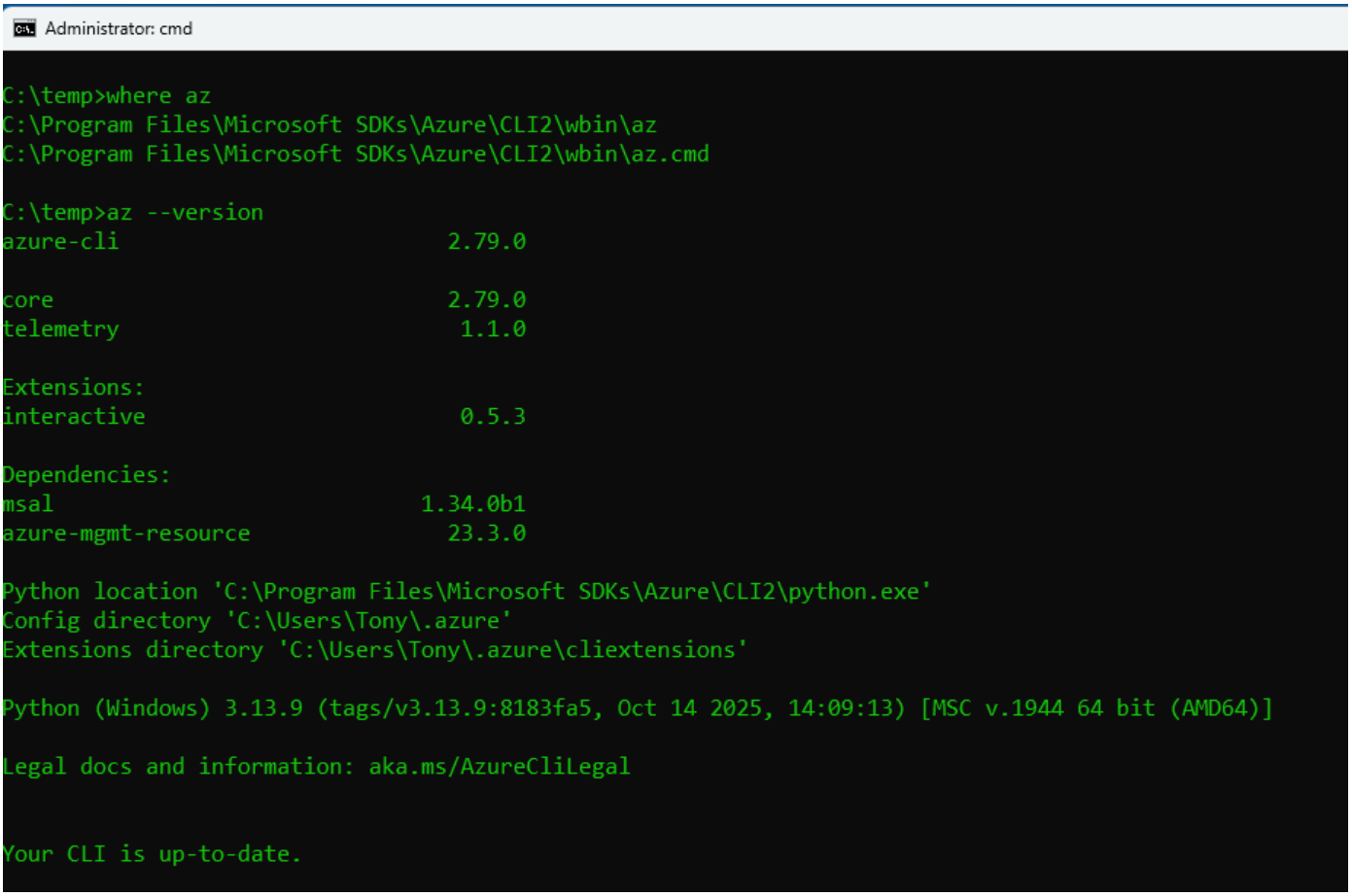
To install the 'Azure CLI', use the following download link:
https://learn.microsoft.com/en-us/cli/azure/install-azure-cli-windows?view=azure-cli-latest&pivots=msi
which will download the ‘installation file’ func-cli-x64.msi (i.e. a Windows installer file).
Run the ‘installation file’ azure-cli-2.79.0-x64.msi as shown in the screenshot below.



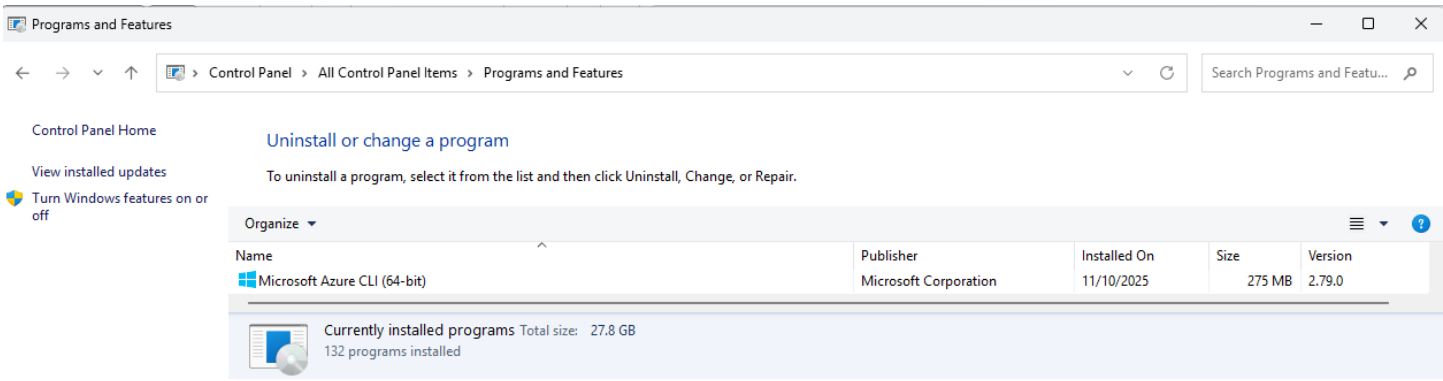
To verify your computer has the 'Azure CLI' version 2.x installed, open a CMD window and issue :

```
az --version
```

as shown in the screenshot below.

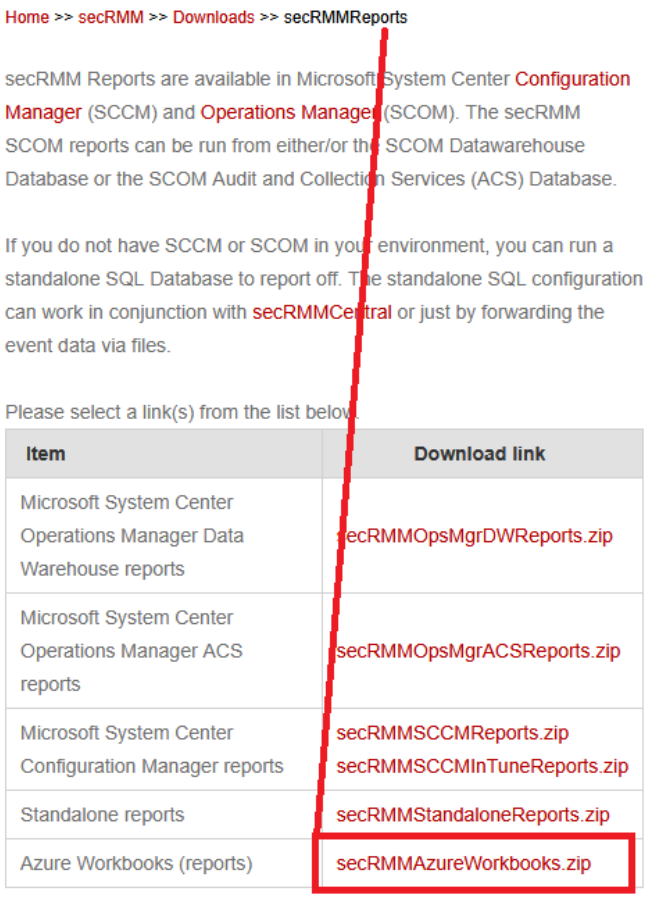


The screenshot below shows the 'Azure CLI' in the installed programs list.



Download secRMM Azure Workbooks

You can download these Azure Workbooks from the Squadra Technologies website:
https://www.squadratechnologies.com/Products/secRMM/secRMMReports.aspx



Home >> secRMM >> Downloads >> secRMMReports

secRMM Reports are available in Microsoft System Center Configuration Manager (SCCM) and Operations Manager (SCOM). The secRMM SCOM reports can be run from either/or the SCOM Datawarehouse Database or the SCOM Audit and Collection Services (ACS) Database.

If you do not have SCCM or SCOM in your environment, you can run a standalone SQL Database to report off. The standalone SQL configuration can work in conjunction with secRMMCentral or just by forwarding the event data via files.

Please select a link(s) from the list below.

Item	Download link
Microsoft System Center Operations Manager Data Warehouse reports	secRMMOpsMgrDWReports.zip
Microsoft System Center Operations Manager ACS reports	secRMMOpsMgrACSReports.zip
Microsoft System Center Configuration Manager reports	secRMMSCCMReports.zip secRMMSCCMInTuneReports.zip
Standalone reports	secRMMStandaloneReports.zip
Azure Workbooks (reports)	secRMMAzureWorkbooks.zip

Once you have downloaded secRMMAzureWorkbooks.zip, extract the zip to a working directory.

Load secRMM Azure Workbooks using PowerShell

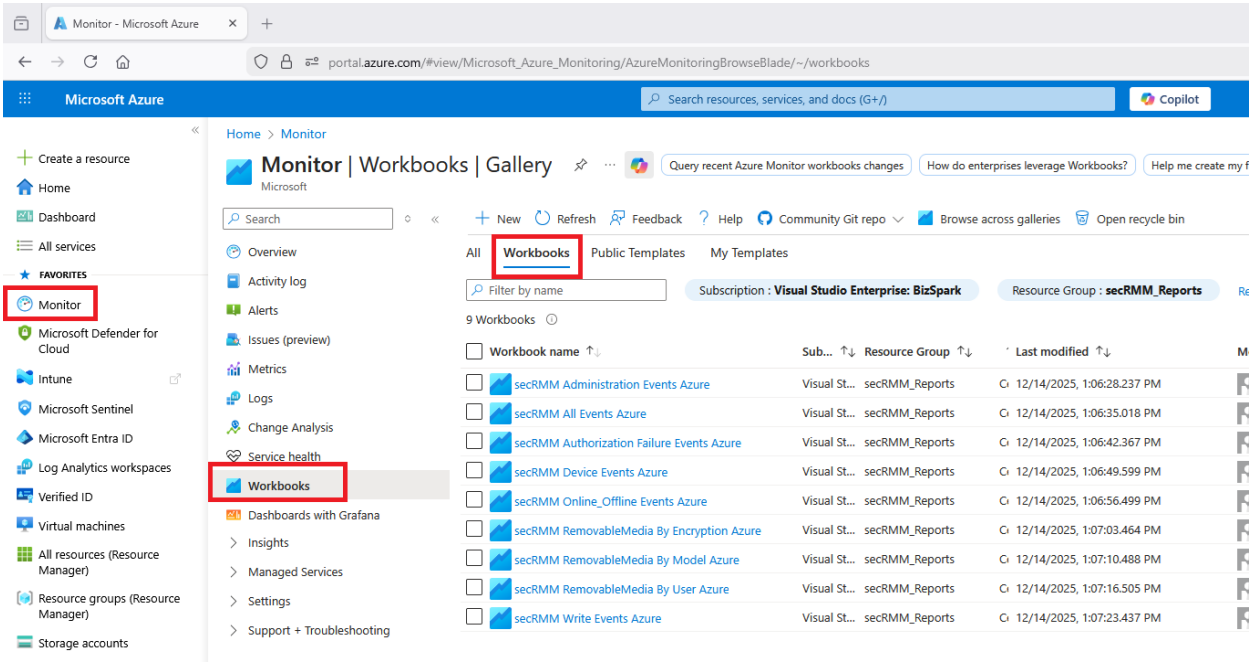
In the working directory where you extracted the zip file from above, go into PowerShell (by typing PowerShell in a CMD window) and then type:
.\ImportsecRMMAzureWorkbooks.ps1

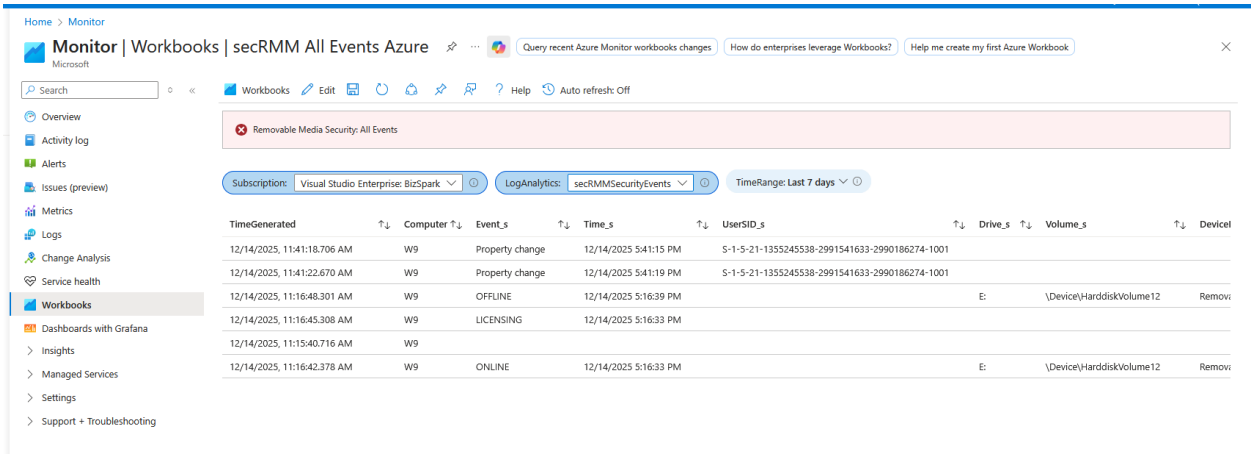
ImportsecRMMAzureWorkbooks.ps1 will prompt you to select:
1. An Azure Subscription (where the workbooks will be associated for billing)
2. An existing or new resource group (for example secRMM_Reports)
3. If you are creating a new resource group in step 2, you will be prompted to select a region to create the new resource group in.

```
PS D:\Projects\Squadra\secRMM\Azure\Monitor> .\ImportsecRMMAzureWorkbooks.ps1
Logged in as: Anthony@anthonysquadratechnologies.onmicrosoft.com
WARNING: A few accounts are skipped as they don't have 'Enabled' state. Use '--all' to display them.
Deploying secRMM Administration Events Azure into resource group secRMM_Reports
Deploying secRMM All Events Azure into resource group secRMM_Reports
Deploying secRMM Authorization Failure Events Azure into resource group secRMM_Reports
Deploying secRMM Device Events Azure into resource group secRMM_Reports
Deploying secRMM Online_Offline Events Azure into resource group secRMM_Reports
Deploying secRMM RemovableMedia By Encryption Azure into resource group secRMM_Reports
Deploying secRMM RemovableMedia By Model Azure into resource group secRMM_Reports
Deploying secRMM RemovableMedia By User Azure into resource group secRMM_Reports
Deploying secRMM Write Events Azure into resource group secRMM_Reports
PS D:\Projects\Squadra\secRMM\Azure\Monitor>
```

Once ImportsecRMMAzureWorkbooks.ps1 completes, the Azure Workbooks are ready to be used in your Azure tenant.

As of December 14, 2025, you can only see the Azure Workbooks in Azure Monitor





Usage

Now that the secRMM security events are going into Azure Log Analytics and Azure Defender for Cloud, we can tell Azure Defender for Cloud what removable storage security events (via secRMM) are important to your security strategy. There are many possibilities. Below, we will show you some samples queries that you can define within your Azure Defender for Cloud instance. If you want help setting up your removable storage security strategy, please feel free to contact Squadra Technologies support (support@squadratechnologies.com).

Azure Defender for Cloud Queries

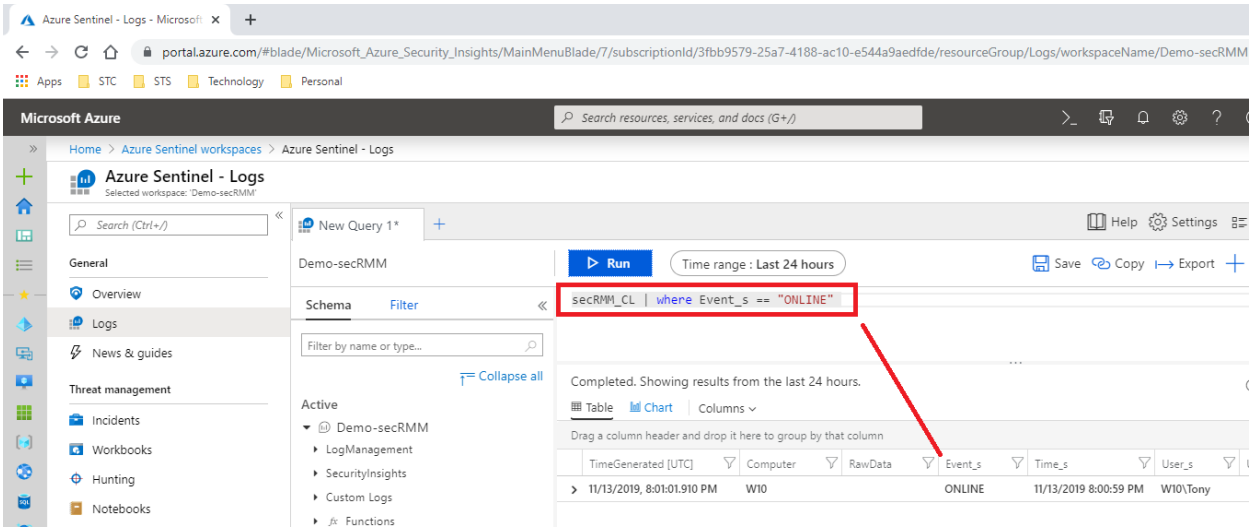
Azure uses a query language named “Keyword Query Language” (KQL). The samples below will show you KQL for the secRMM security events.

Sample query 1 – ONLINE events

When a removable storage device gets USB attached to a Windows computer, secRMM will generate an ONLINE (event id 400). This event tells you who (possibly more than one) is logged into the Windows computer and all the properties about the removable storage device (even if it is a mobile device!).

The KQL for this query is:

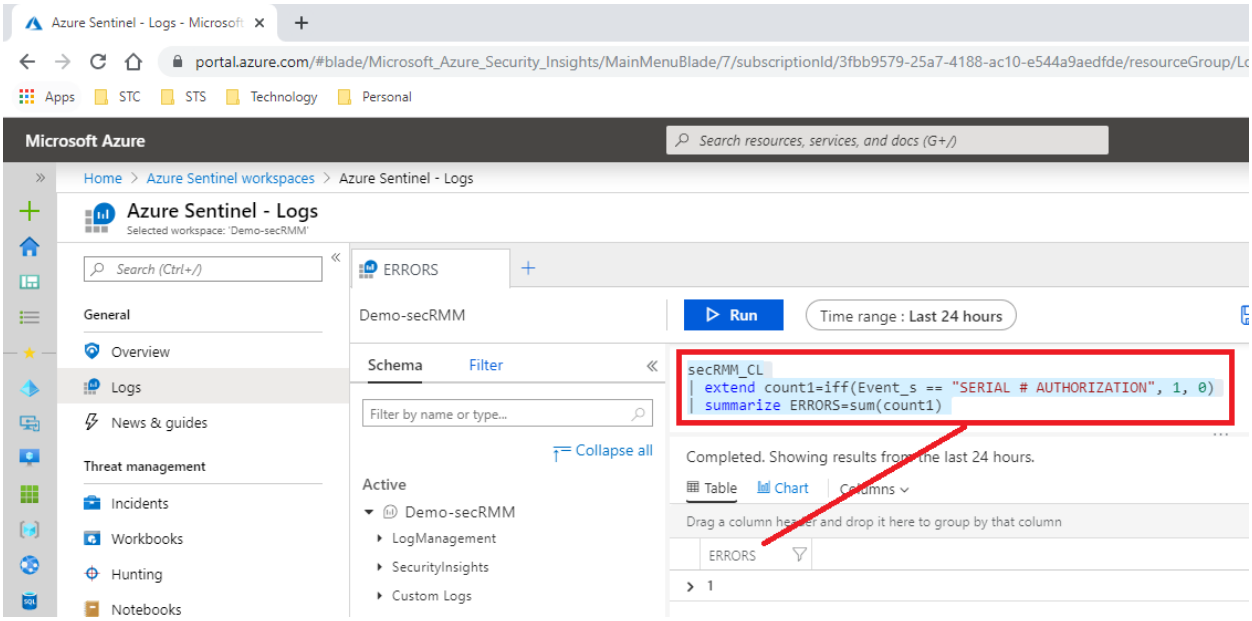
```
secRMM_CL | where Event_s == "ONLINE"
```



Sample query 2 – Count the number of failed write attempts events

secRMM has policies (rules) that can allow your end-users to read from removable storage but not the ability to write to removable storage. If you want to total up how many times a user has attempted to write to a removable storage device but was prevented from writing due to secRMM, the KQL query is:

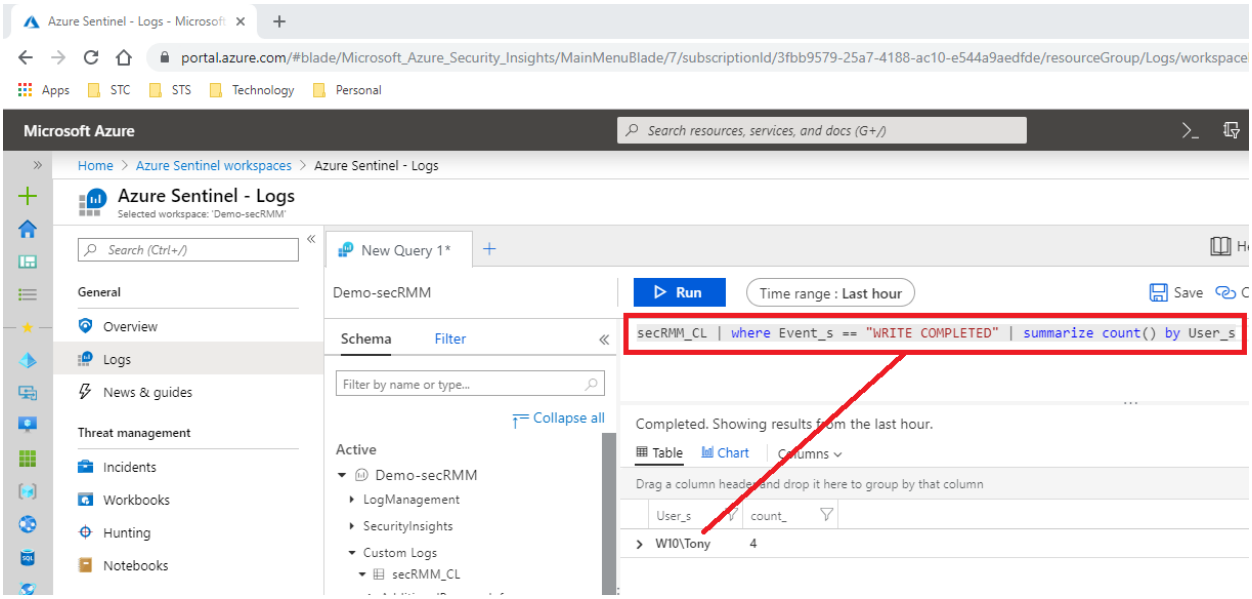
```
secRMM_CL
| extend count1=iff(Event_s == "SERIAL # AUTHORIZATION", 1, 0)
| summarize ERRORS=sum(count1)
```



Sample query 3 – Which users are writing files to removable storage devices

secRMM generates a security event for every file that is written to a removable storage device. If you want see which users and how many files each user is writing to removable storage, the KQL query is:

```
secRMM_CL | where Event_s == "WRITE COMPLETED" | summarize count() by User_s
```



Sample query 4 – Which users attempted writing files to removable storage devices but failed

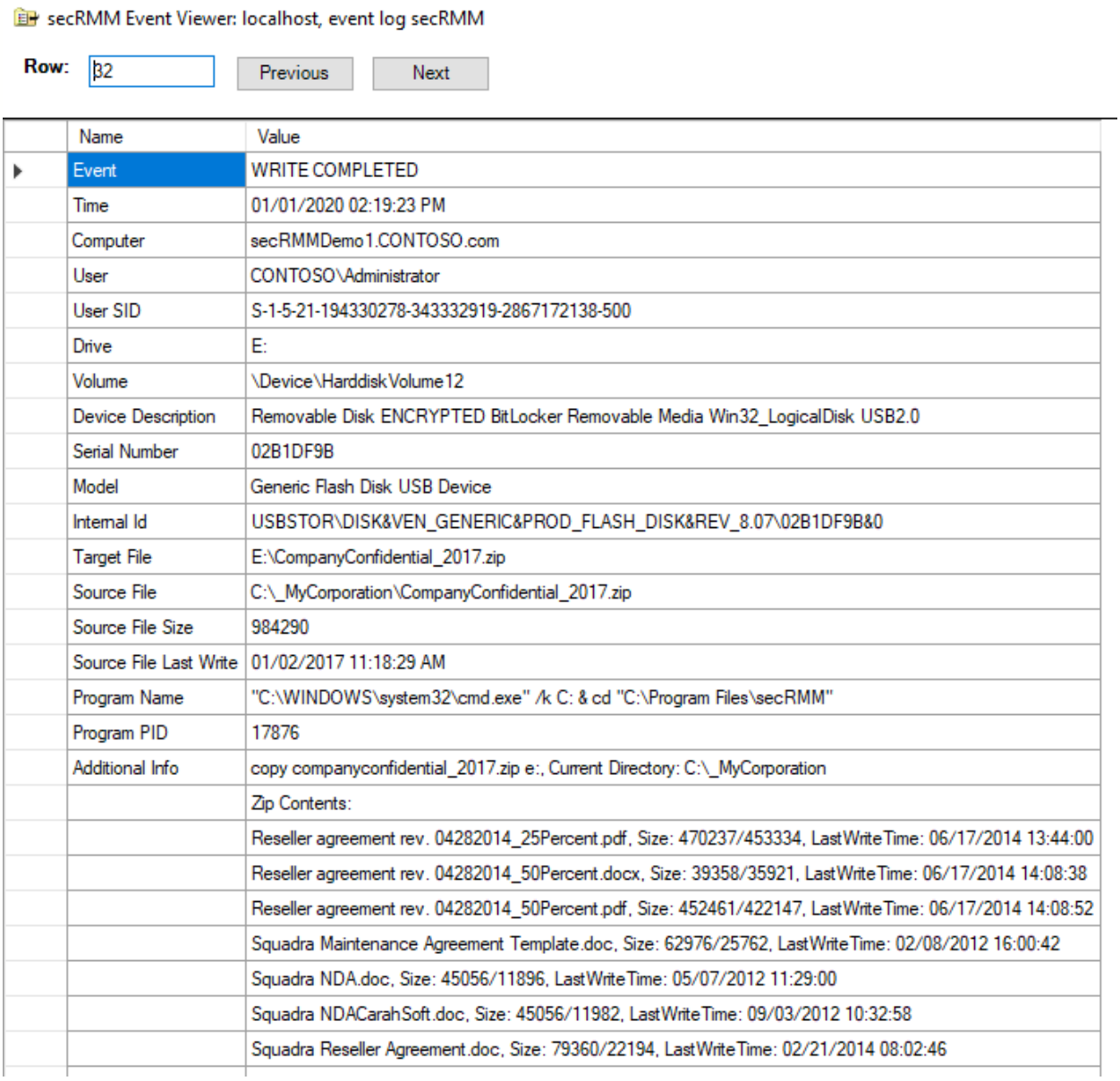
secRMM generates a security event for every file write attempt to a removable storage device that fails due to a security policy. If you want see which users and how many files each user is writing to removable storage, the KQL query is:

```
secRMM_CL | where Event_s contains "AUTHORIZATION" | where TimeGenerated > ago(1d) | summarize count() by User_s | render barchart
```

More sample queries

Microsoft BitLocker Activity for removable storage devices

```
secRMM_CL | where DeviceDescription_s contains "ENCRYPTED BitLocker"
```



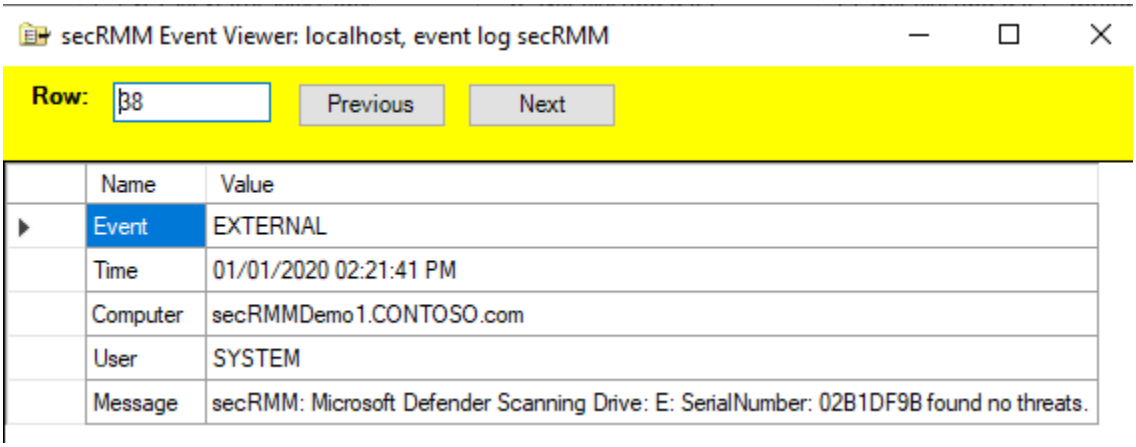
secRMM Event Viewer: localhost, event log secRMM

Row: 32 Previous Next

	Name	Value
▶	Event	WRITE COMPLETED
	Time	01/01/2020 02:19:23 PM
	Computer	secRMMDemo1.CONTOSO.com
	User	CONTOSO\Administrator
	User SID	S-1-5-21-194330278-343332919-2867172138-500
	Drive	E:
	Volume	\Device\HarddiskVolume12
	Device Description	Removable Disk ENCRYPTED BitLocker Removable Media Win32_LogicalDisk USB2.0
	Serial Number	02B1DF9B
	Model	Generic Flash Disk USB Device
	Internal Id	USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\02B1DF9B&0
	Target File	E:\CompanyConfidential_2017.zip
	Source File	C:_MyCorporation\CompanyConfidential_2017.zip
	Source File Size	984290
	Source File Last Write	01/02/2017 11:18:29 AM
	Program Name	"C:\WINDOWS\system32\cmd.exe" /k C: & cd "C:\Program Files\secRMM"
	Program PID	17876
	Additional Info	copy companyconfidential_2017.zip e:, Current Directory: C:_MyCorporation
		Zip Contents:
		Reseller agreement rev. 04282014_25Percent.pdf, Size: 470237/453334, LastWriteTime: 06/17/2014 13:44:00
		Reseller agreement rev. 04282014_50Percent.docx, Size: 39358/35921, LastWriteTime: 06/17/2014 14:08:38
		Reseller agreement rev. 04282014_50Percent.pdf, Size: 452461/422147, LastWriteTime: 06/17/2014 14:08:52
		Squadra Maintenance Agreement Template.doc, Size: 62976/25762, LastWriteTime: 02/08/2012 16:00:42
		Squadra NDA.doc, Size: 45056/11896, LastWriteTime: 05/07/2012 11:29:00
		Squadra NDACarahSoft.doc, Size: 45056/11982, LastWriteTime: 09/03/2012 10:32:58
		Squadra Reseller Agreement.doc, Size: 79360/22194, LastWriteTime: 02/21/2014 08:02:46

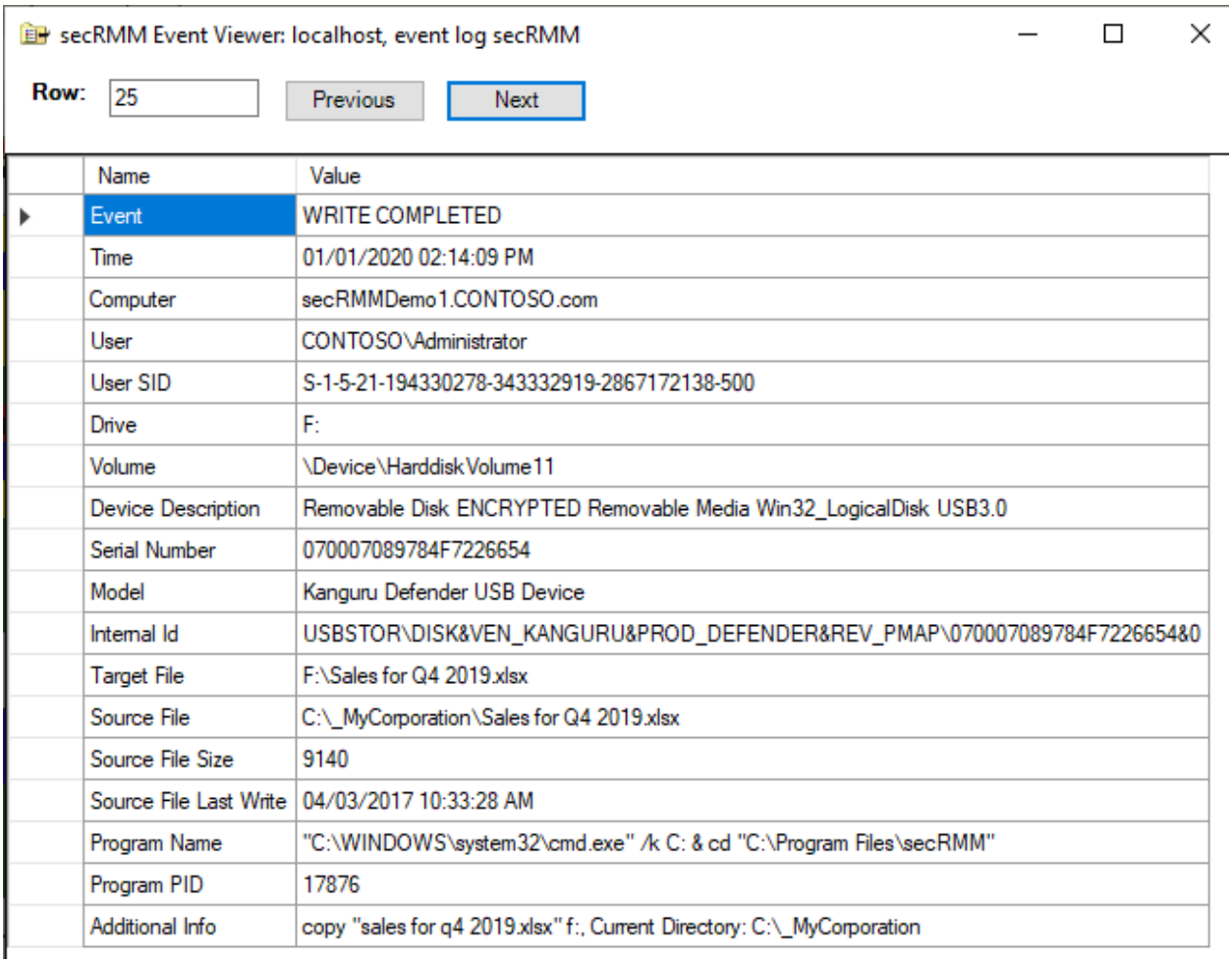
Microsoft Windows Defender Activity for removable storage devices

```
secRMM_CL | where ((Event_s == "EXTERNAL") and (Message contains "Microsoft Defender"))
```



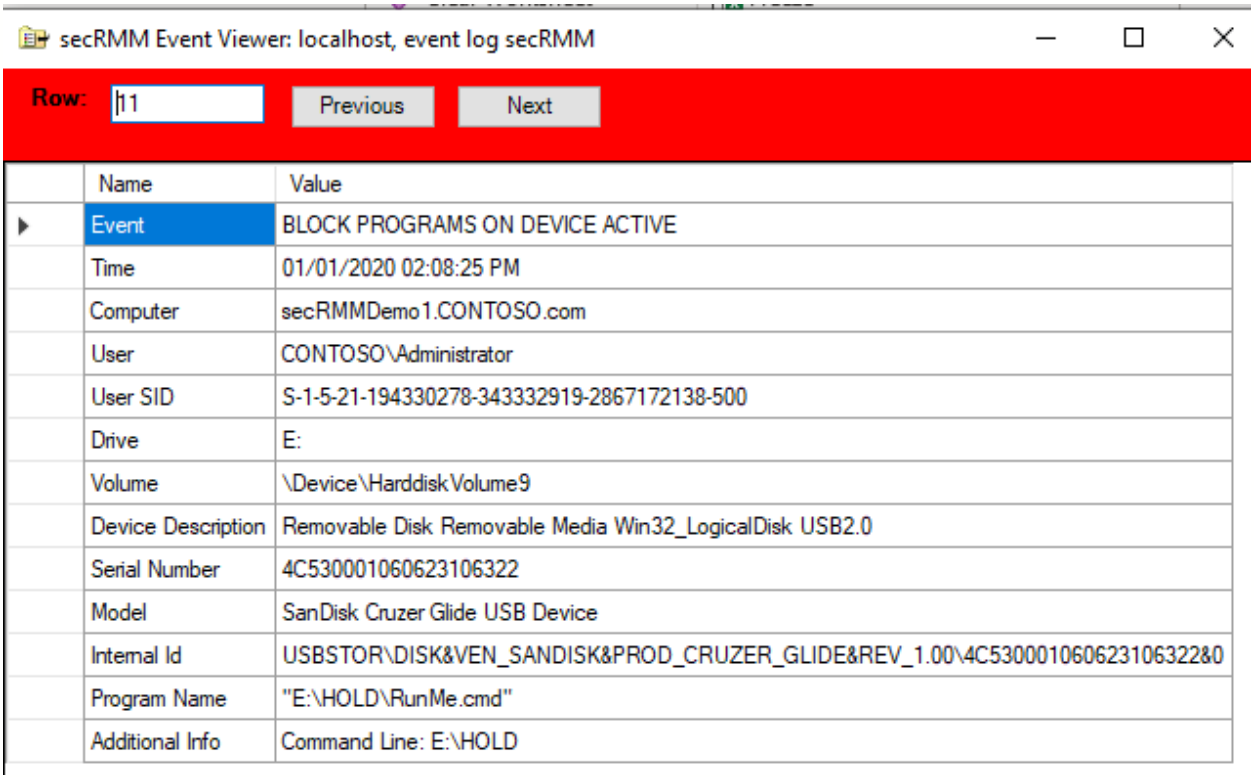
Hardware Encrypted Device Activity

```
secRMM_CL | where DeviceDescription_s contains " ENCRYPTED Removable Media"
```



Users who have tried to execute macros or programs from a removable storage device

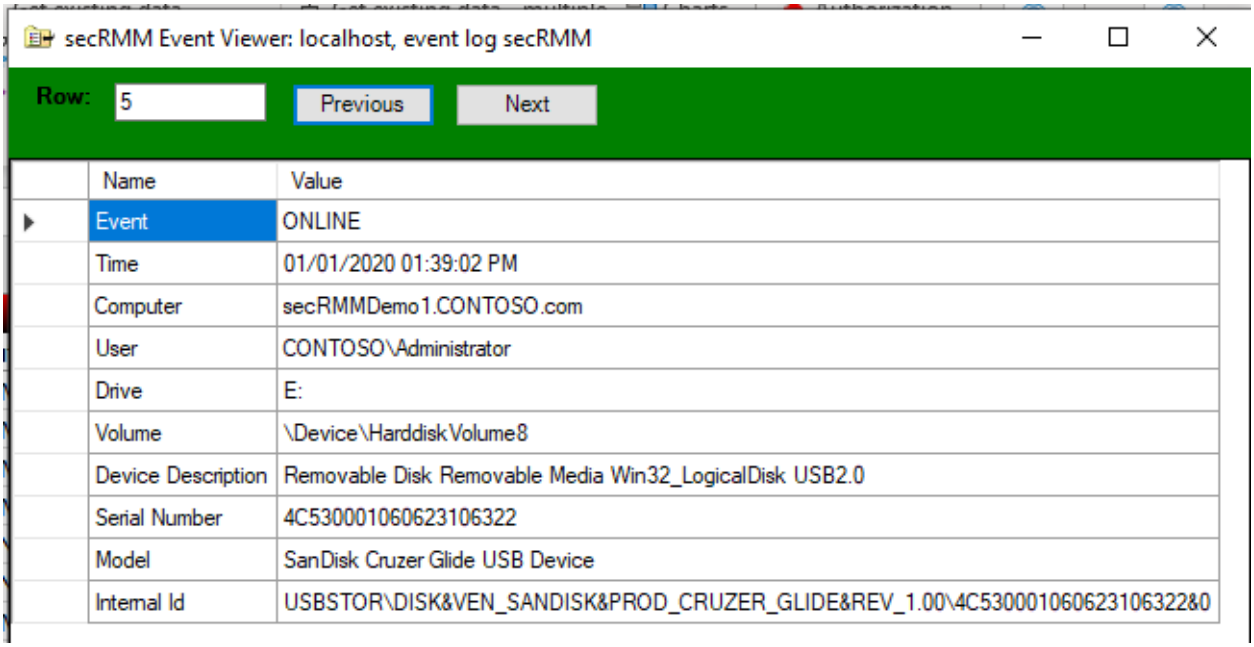
```
secRMM_CL | where ((Event_s == "BLOCK MACROS ON DEVICE ACTIVE") or (Event_s ==
"BLOCK PROGRAMS ON DEVICE ACTIVE")) | summarize count() by User_s
```



	Name	Value
▶	Event	BLOCK PROGRAMS ON DEVICE ACTIVE
	Time	01/01/2020 02:08:25 PM
	Computer	secRMMDemo1.CONTOSO.com
	User	CONTOSO\Administrator
	User SID	S-1-5-21-194330278-343332919-2867172138-500
	Drive	E:
	Volume	\Device\HarddiskVolume9
	Device Description	Removable Disk Removable Media Win32_LogicalDisk USB2.0
	Serial Number	4C530001060623106322
	Model	SanDisk Cruzer Glide USB Device
	Internal Id	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_GLIDE&REV_1.00\4C530001060623106322&0
	Program Name	"E:\HOLD\RunMe.cmd"
	Additional Info	Command Line: E:\HOLD

Removable storage devices that are not encrypted (hardware or software)

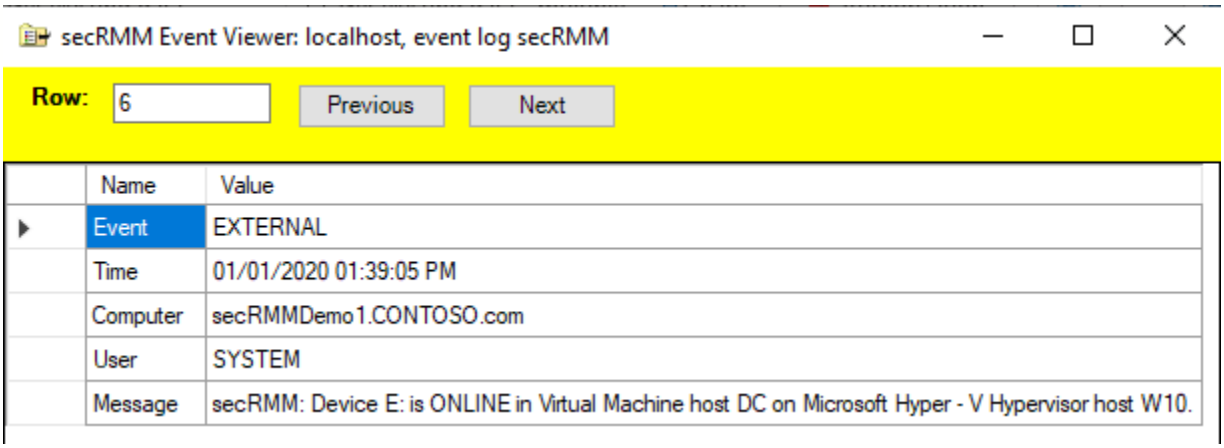
```
secRMM_CL | where ((Event_s == "ONLINE") and (DeviceDescription_s !contains
"ENCRYPTED"))
```



Removable storage devices that are mounted into a Virtual Machine

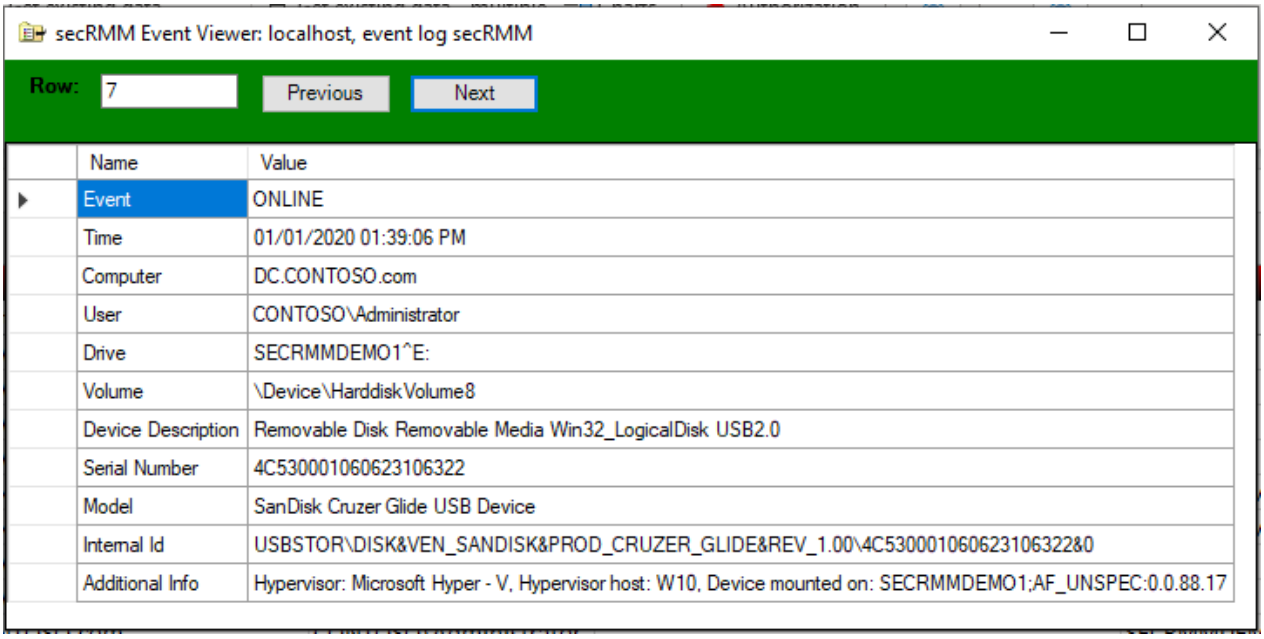
Event on the physical machine

```
secRMM_CL | where ((Event_s == "EXTERNAL") and (Message contains "ONLINE") and
(Message contains "Virtual Machine"))
```



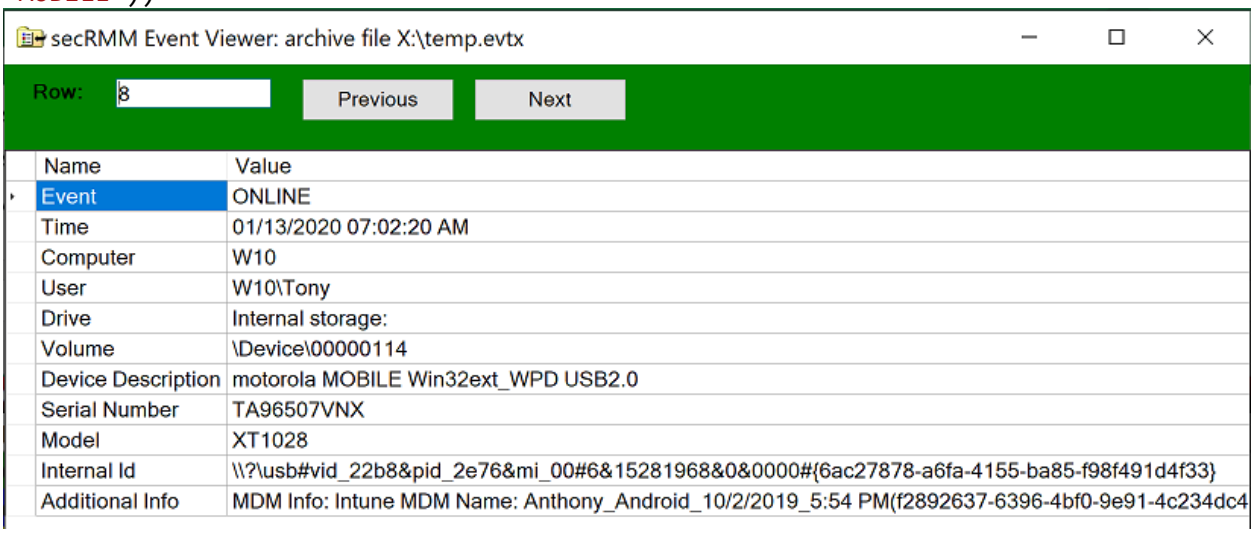
Event on the virtual machine

```
secRMM_CL | where ((Event_s == "ONLINE") and (Drive_s contains "^"))
```



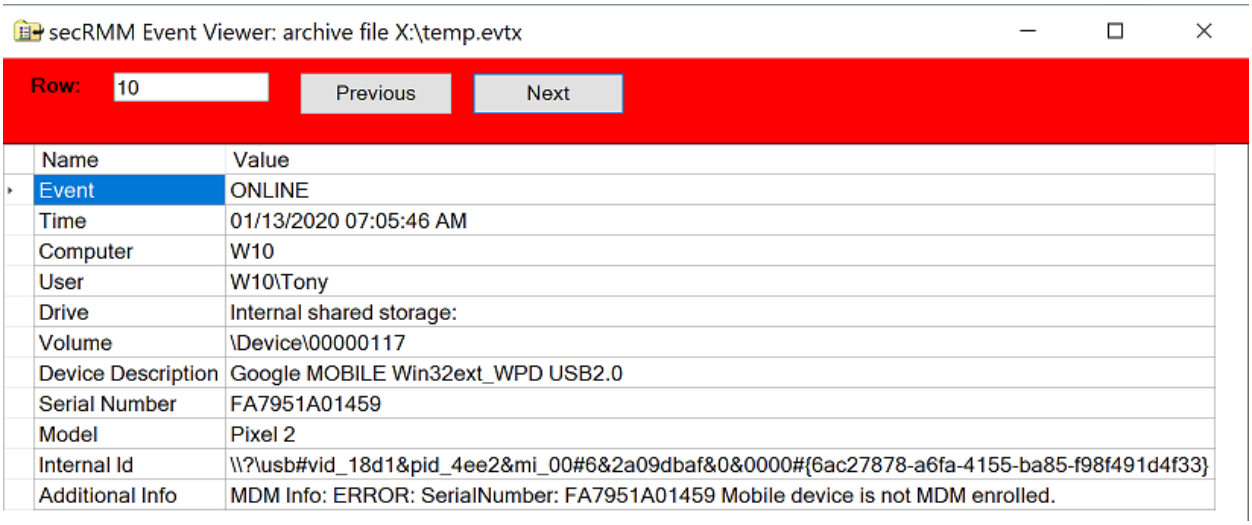
Show mobile devices that are being USB mounted

```
secRMM_CL | where ((Event_s == "ONLINE") and (DeviceDescription_s contains
"MOBILE"))
```



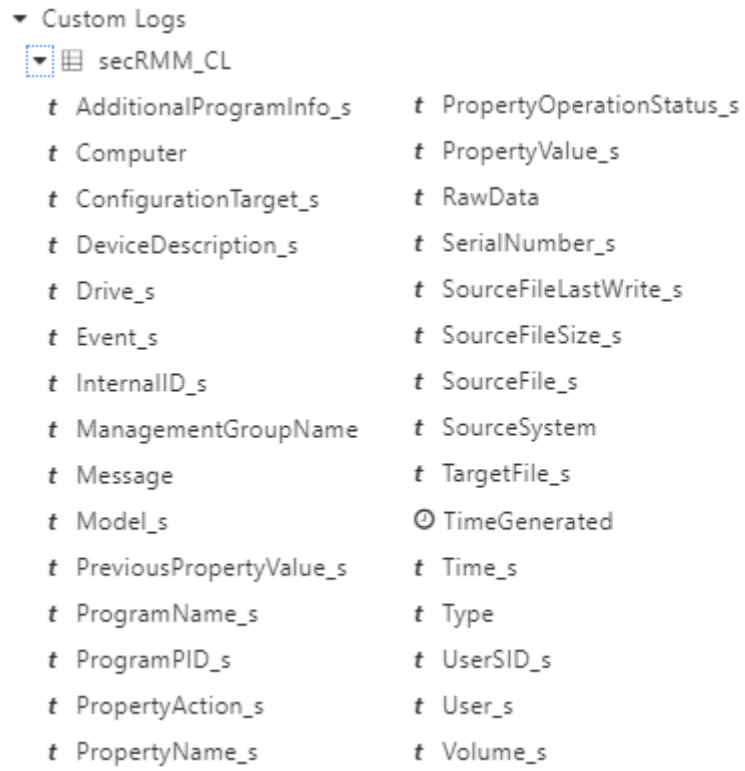
Show mobile devices that are being USB mounted but are not MDM (Microsoft Intune) enrolled

```
secRMM_CL | where ((Event_s == "ONLINE") and (AdditionalProgramInfo_s contains
"Mobile device is not MDM enrolled"))
```



Azure Log Analytics secRMM schema

This section explains the fields (columns) that are available on the secRMM Log Analytics table.



Descriptions

Additional Program Info	Additional program information (used in cmd.exe, powershell, vbscript and jscript programs).

Computer	The computer where the event occurred. For the secRMM event log, this will always list the same computer. For secRMMCentral, it will have all the computers that are forwarding their secRMM events into the secRMMCentral event log.
Configuration Target	The name of the secRMM configuration which is either a computer or user configuration (policy).
Device Description	The removable media device description.
Drive	The drive letter of the removable media device.
Event	This is the event ID translated into meaningful text.
Internal ID	The internal ID of the removable media device.
Message	Any additional information secRMM generates for the event
Model	The manufacturer model of the removable media device.
Previous Property Value	For Administration events, the previous value of the property.
Program Name	The name of the program used to perform the write operation to the removable media device.
Program PID	The program PID.
Property Action	For Administration events, the action taken on the property involved in the event.
Property Name	For Administration events, the name of the property involved in the event.
Property Operation Status	For Administration events, the outcome of the event (i.e. successful or unsuccessful).
Property Value	For Administration events, the value of the property.
Serial Number	The removable media device's serial number.
Source File	The source file involved in the write operation to the removable media device.
Source File Last Write	The source file date and time that it was last written to.
Source File Size	The source file size in bytes.
Target File	The name of the file as it is stored on the removable media device.
Time	The date and time the event occurred.
User	The user that is associated with the event.
User SID	The user SID that is associated with the event.
Volume	The volume name of the removable media device.

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, 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, MO 64734 USA
Web site	http://www.squadratechnologies.com/