Security Removable Media Manager

connector to

Microsoft Sentinel

Version 9.11.55.0

(November 2026)

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, MO 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 Excel AddIn Administrator Guide
Created - August 2011

Contents

INTRODUCTION **4**

DESCRIPTION 4
WHY INTEGRATE SECRMM SECURITY EVENTS INTO MICROSOFT SENTINEL? 5

CONFIGURATION **5**

PREREQUISITES 5
CREATE "AZURE LOG WORKSPACE FOR SECRMM" 6
CONNECT "AZURE LOG WORKSPACE FOR SECRMM" TO MICROSOFT SENTINEL 6
LOADING SECRMM AZURE WORKBOOKS FOR TABULAR REPORTING 15
Prerequisites *15*
Azure CLI 15
Download secRMM Azure Workbooks 16
Load secRMM Azure Workbooks using PowerShell 17

USAGE **19**

MICROSOFT SENTINEL QUERIES 19
Sample query 1 – ONLINE events *19*
Sample query 2 – Count the number of failed write attempts events *19*
Sample query 3 – Which users are writing files to removable storage devices *20*
Sample query 4 – Which users attempted writing files to removable storage devices but failed *21*
More sample queries *21*
Microsoft BitLocker Activity for removable storage devices 21
Microsoft Windows Defender Activity for removable storage devices 22
Hardware Encrypted Device Activity 23
Users who have tried to execute macros or programs from a removable storage device 23
Removable storage devices that are not encrypted (hardware or software) 24
Removable storage devices that are mounted into a Virtual Machine 25
Event on the physical machine 25
Event on the virtual machine 25
Show mobile devices that are being USB mounted 25
Show mobile devices that are being USB mounted but are not MDM (Microsoft Intune) enrolled 26
MICROSOFT SENTINEL WORKBOOK 26
MICROSOFT SENTINEL ANALYTICS 27
AZURE LOG ANALYTICS SECRMM SCHEMA 33
Descriptions *33*

CONTACTING SQUADRA TECHNOLOGIES SUPPORT **34**

ABOUT SQUADRA TECHNOLOGIES, LLC. **34**

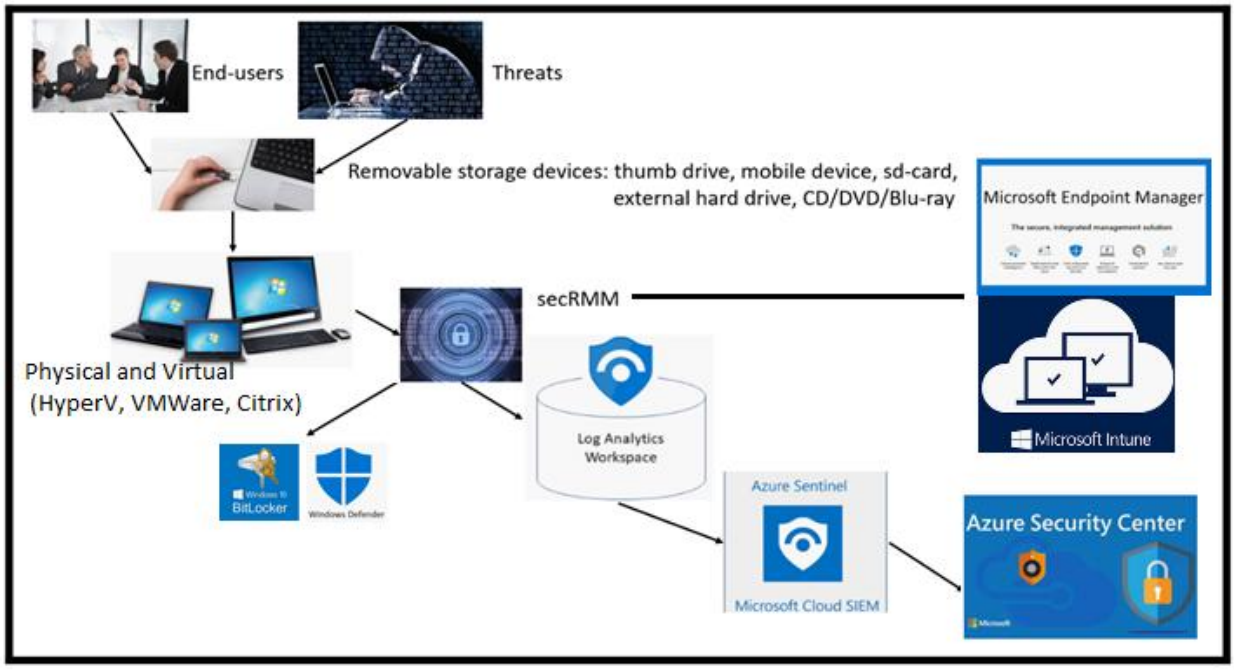
Introduction

Description

Microsoft Sentinel makes it easy to collect security data across your entire hybrid organization from devices, to users, to apps, to servers on any cloud. It uses the power of artificial intelligence to ensure you are identifying real threats quickly and unleashes you from the burden of traditional SIEMs by eliminating the need to spend time on setting up, maintaining, and scaling infrastructure. Since it is built on Azure, it offers nearly limitless cloud scale and speed to address your security needs. Traditional SIEMs have also proven to be expensive to own and operate, often requiring you to commit upfront and incur high cost for infrastructure maintenance and data ingestion. With Microsoft Sentinel there are no upfront costs, you pay for what you use.

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 Sentinel instance. This allows you to see the security events that secRMM generates within Sentinel. 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 Microsoft Sentinel" to refer to this secRMM to Microsoft Microsoft Sentinel integration.



If you follow the steps in this document, it should take no more than 20 minutes to be up and running.

Why integrate secRMM security events into Microsoft Sentinel?

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 Sentinel as your centralized security tool, 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.

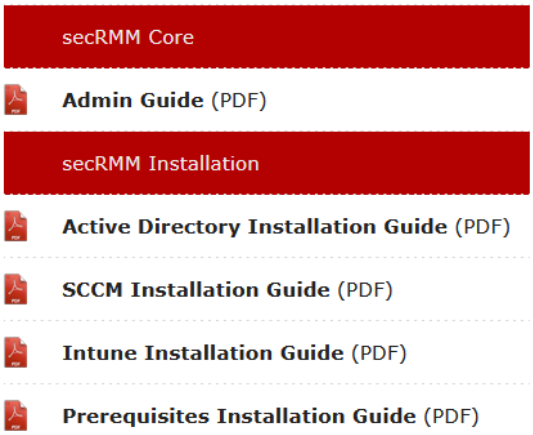
Configuration

Prerequisites

To use the "secRMM Connector to Microsoft Sentinel", 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).



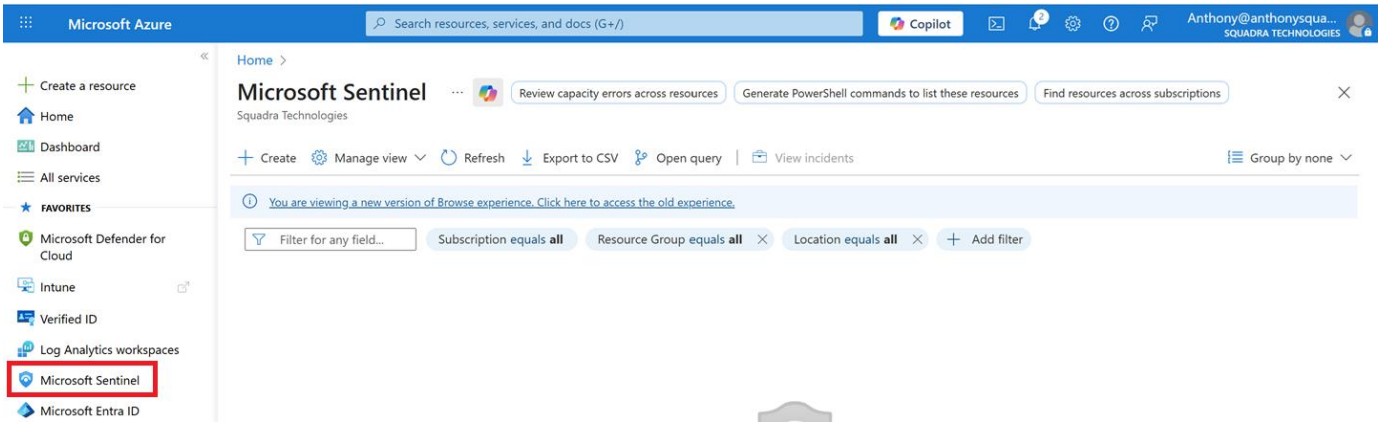
Create "Azure Log Workspace for secRMM"

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.

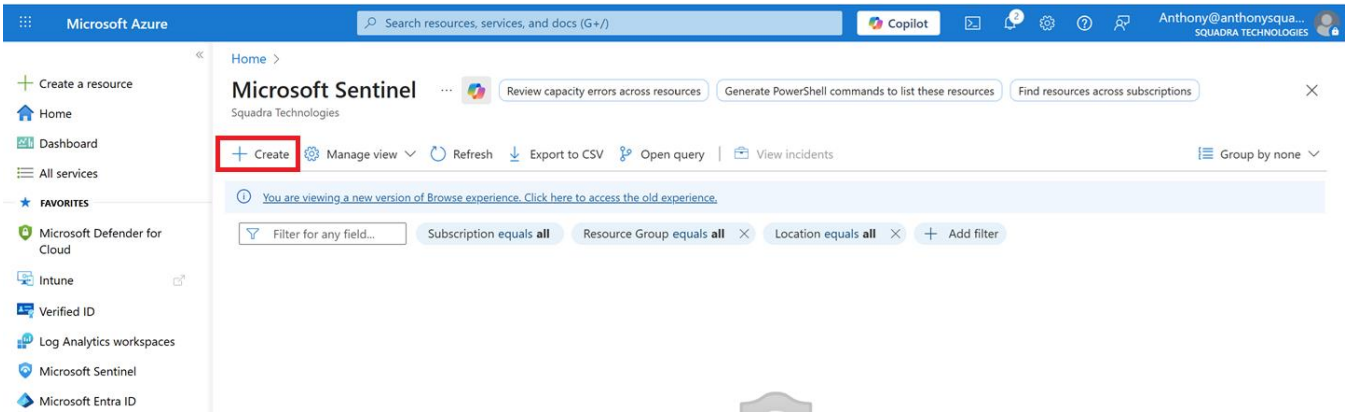
Connect "Azure Log Workspace for secRMM" to Microsoft Sentinel

Now that you have created a "Azure Log Workspace for secRMM" (from the section above), you will connect the "Azure Log Workspace for secRMM" to your Microsoft Sentinel instance.

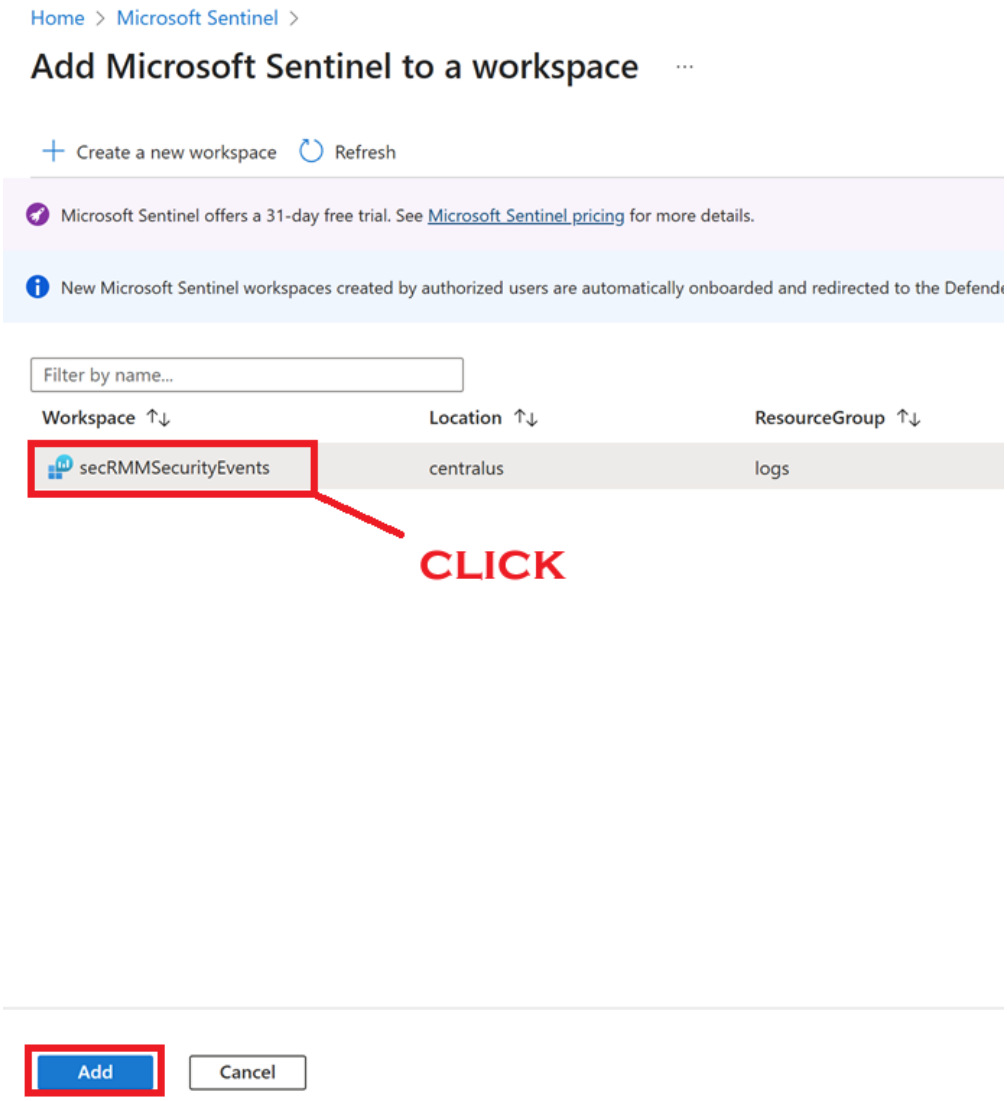
From your Azure portal, go to your 'Microsoft Sentinel' instance (as shown in the screenshot below).



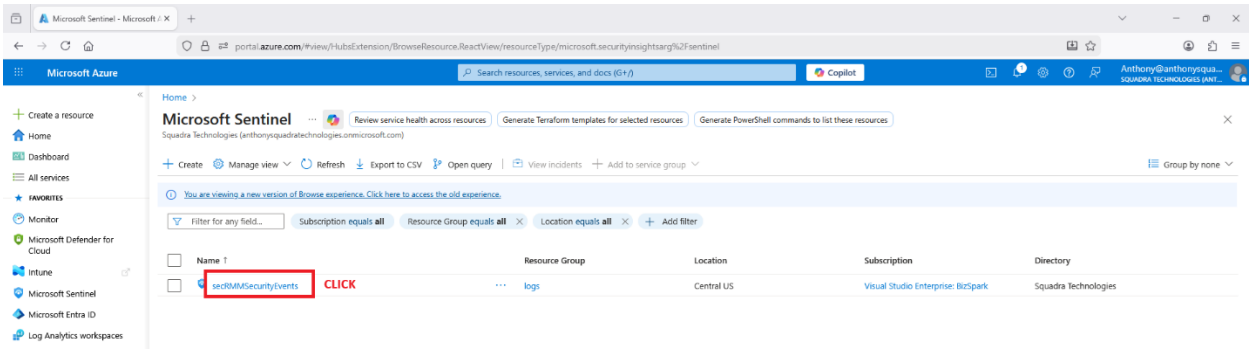
Click the Create link (as shown in the screenshot below).



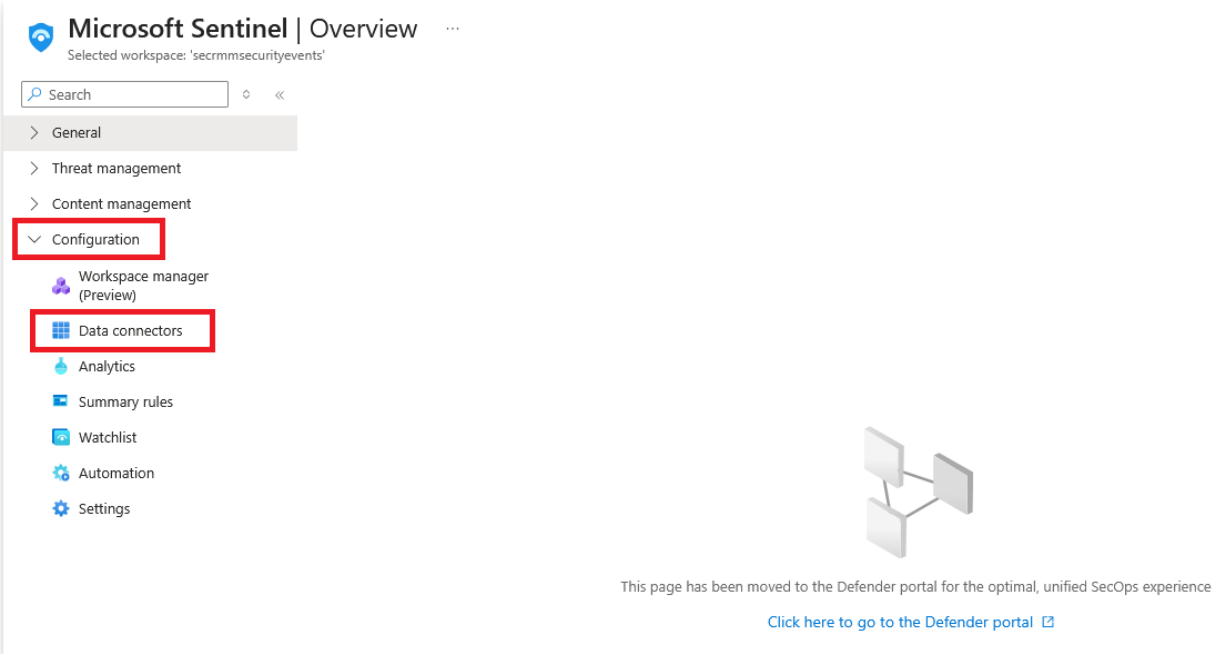
Select the workspace (i.e. the “Azure Log Workspace for secRMM”) you created in the previous subsection (as shown in the screenshot below).



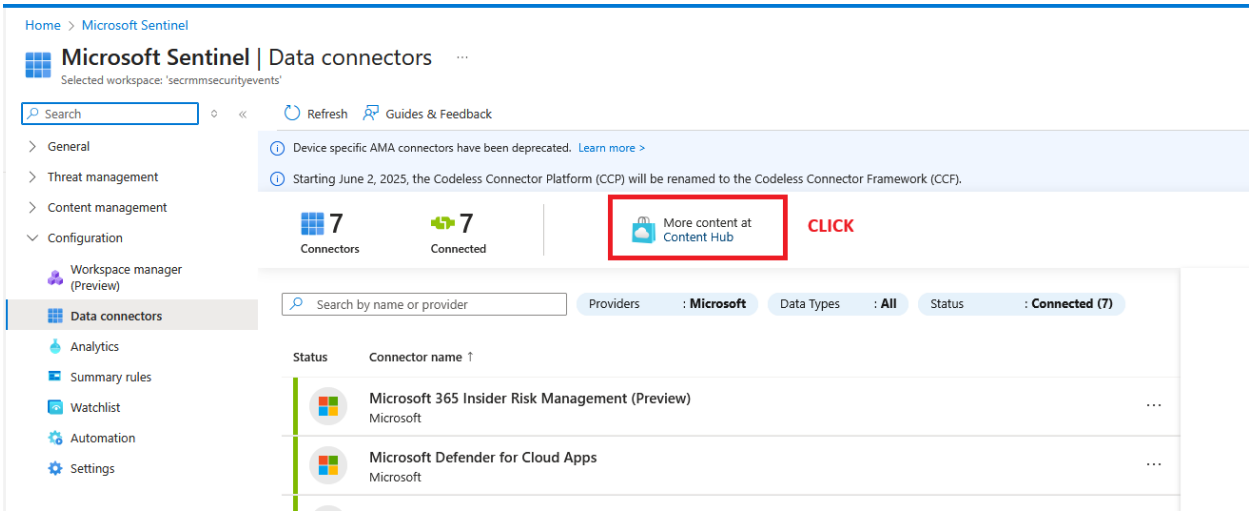
Now click the workspace as shown in the screenshot below.



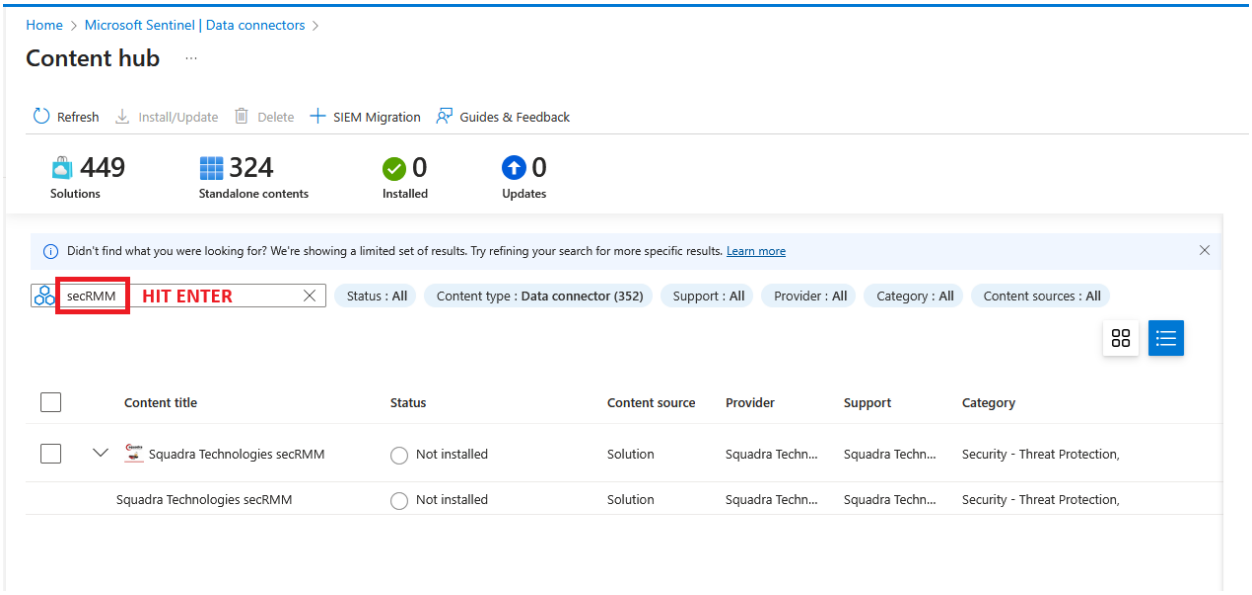
Under Configuration, click ‘Data connectors’ as shown in the screenshot below.



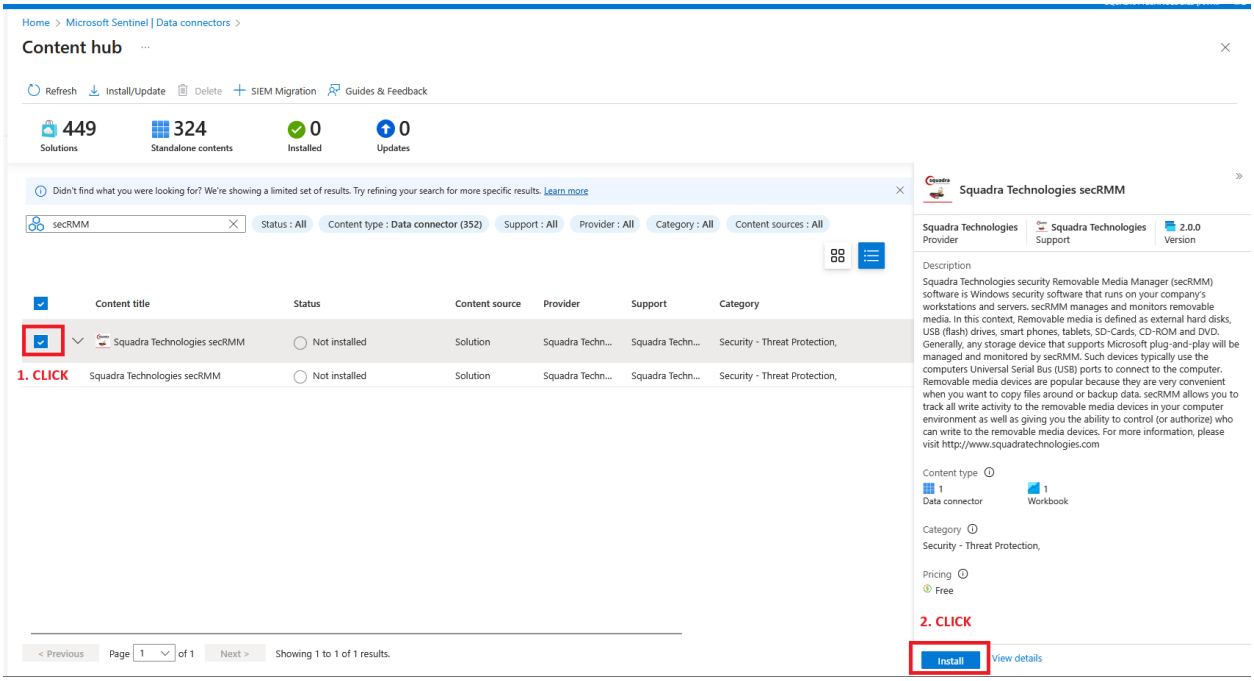
Click the ‘Content Hub’ link as shown in the screenshot below.



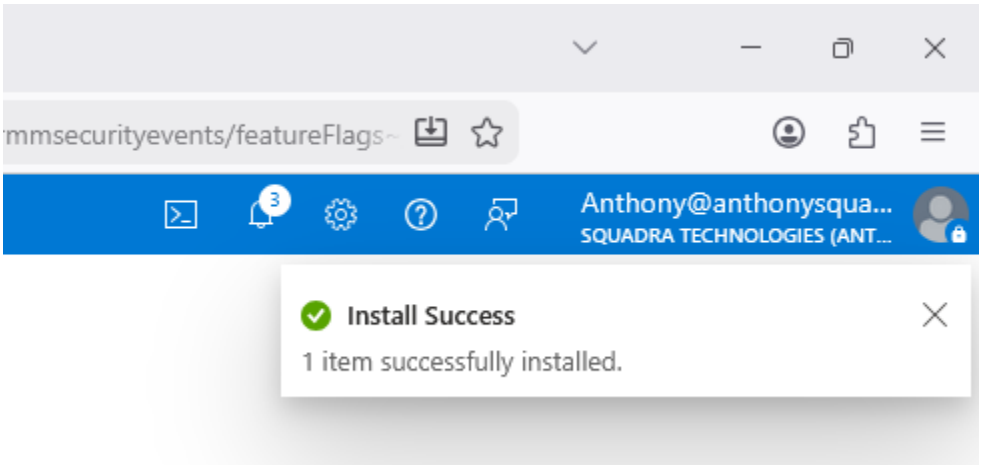
Set a filter for “secRMM” as shown in screenshot below.



Select the ‘Squadra Technologies secRMM’ checkbox and then click the install button as shown in the screenshot below.

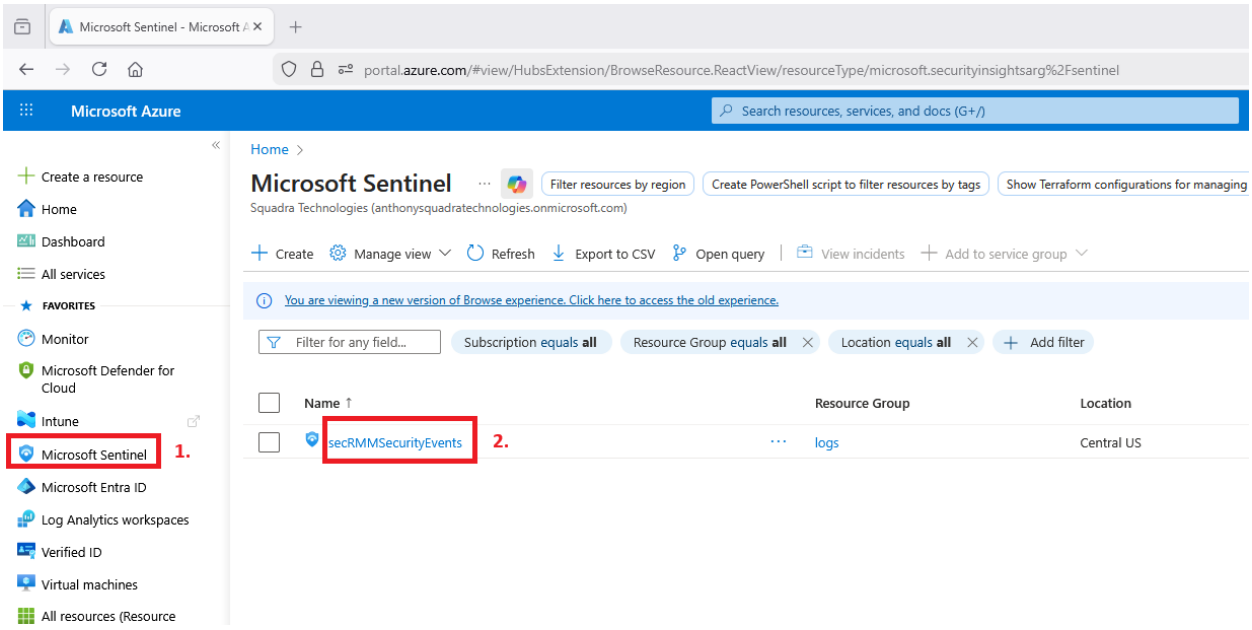


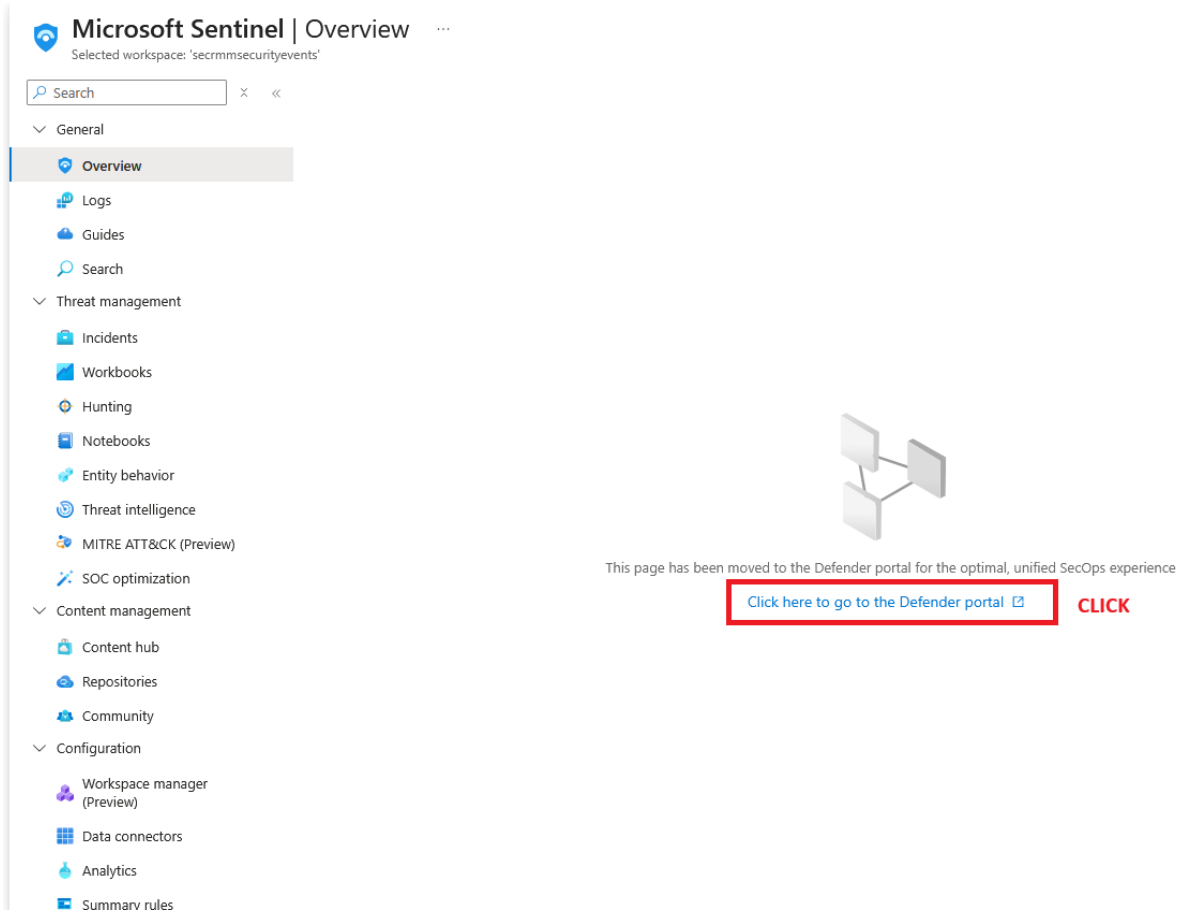
In the upper right corner of the browser, you will see an 'Install Success' message as shown in the screenshot below.



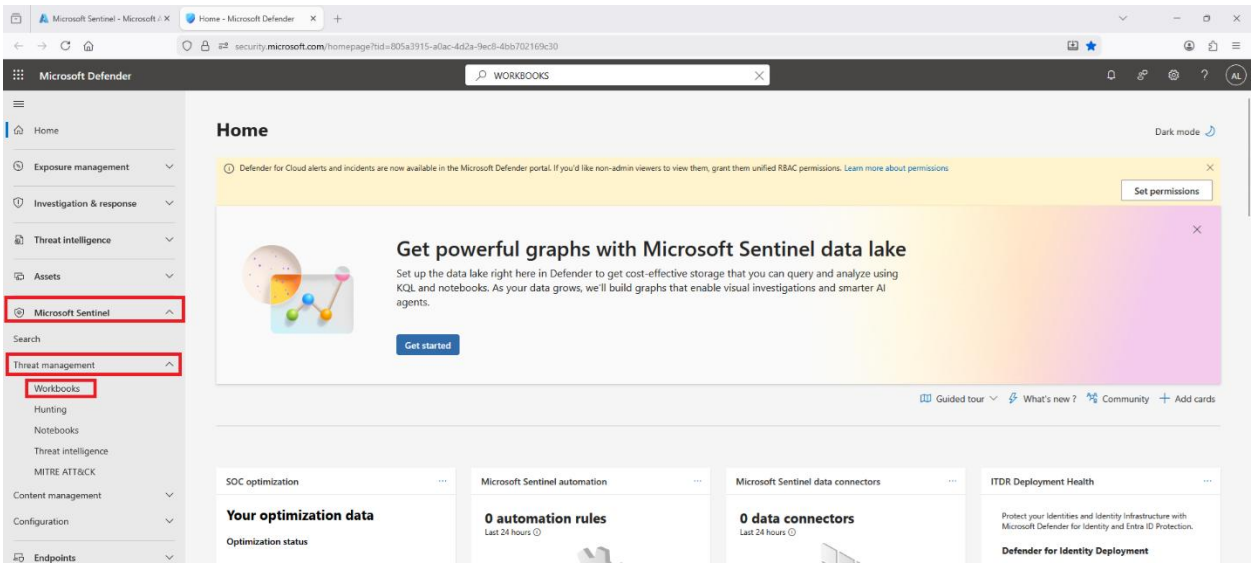
As of December 11, 2025, Microsoft has changed 'Microsoft Sentinel' to be integrated with 'Defender Portal'.

Now that you have connected the "Squadra Technologies secRMM Data Connector" to your Microsoft Sentinel instance, we need to save the secRMM Workbook.

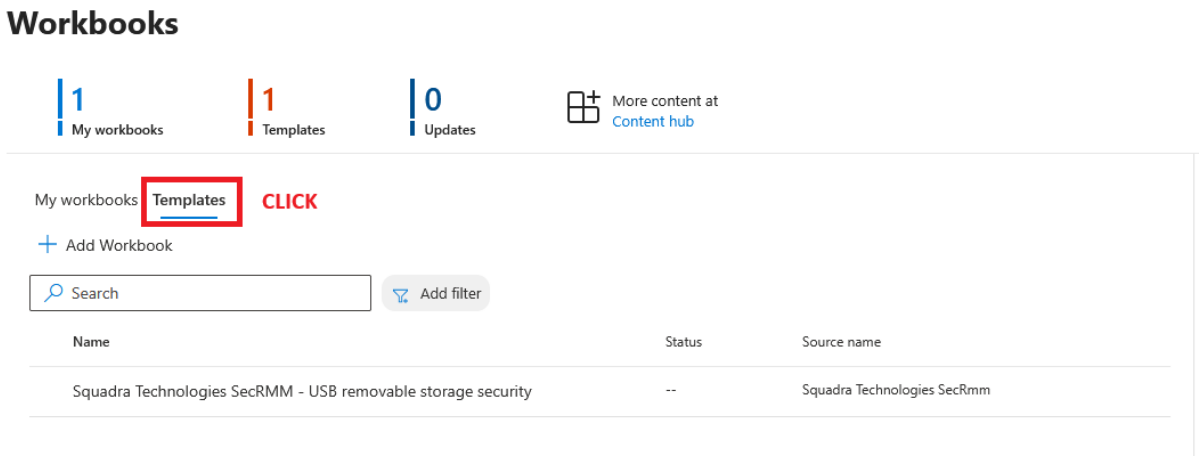

Microsoft Sentinel - Microsoft
portal.azure.com/#view/HubsExtension/BrowseResource.ReactView/resourceType/microsoft.securityinsightsarg%2Fsentinel
Microsoft Azure
Search resources, services, and docs (G+/)
Create a resource
Home
Dashboard
All services
FAVORITES
Monitor
Microsoft Defender for Cloud
Intune
Microsoft Sentinel
1.
Microsoft Entra ID
Log Analytics workspaces
Verified ID
Virtual machines
All resources (Resource
Home
Microsoft Sentinel
Squadra Technologies (anthonysquadratechnologies.onmicrosoft.com)
Filter resources by region
Create PowerShell script to filter resources by tags
Show Terraform configurations for managing
Create
Manage view
Refresh
Export to CSV
Open query
View incidents
Add to service group
You are viewing a new version of Browse experience. Click here to access the old experience.
Filter for any field...
Subscription equals all
Resource Group equals all
Location equals all
Add filter
Name
Resource Group
Location
secRMMSecurityEvents
2.
logs
Central US


Microsoft Sentinel | Overview
Selected workspace: 'secrmmsecurityevents'
Search
General
Overview
Logs
Guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules
This page has been moved to the Defender portal for the optimal, unified SecOps experience
Click here to go to the Defender portal
CLICK

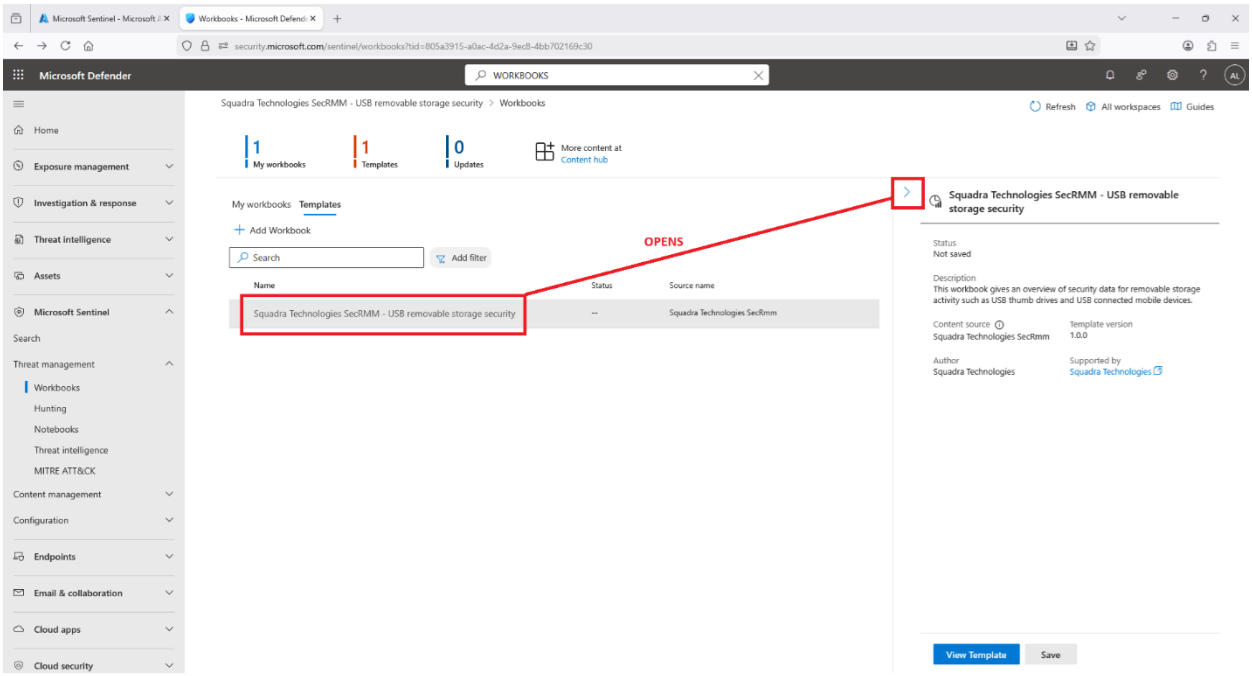
On the left blade (column), go under ‘Microsoft Sentinel’, ‘Threat management’ and click ‘Workbooks’ as shown in the screenshot below.



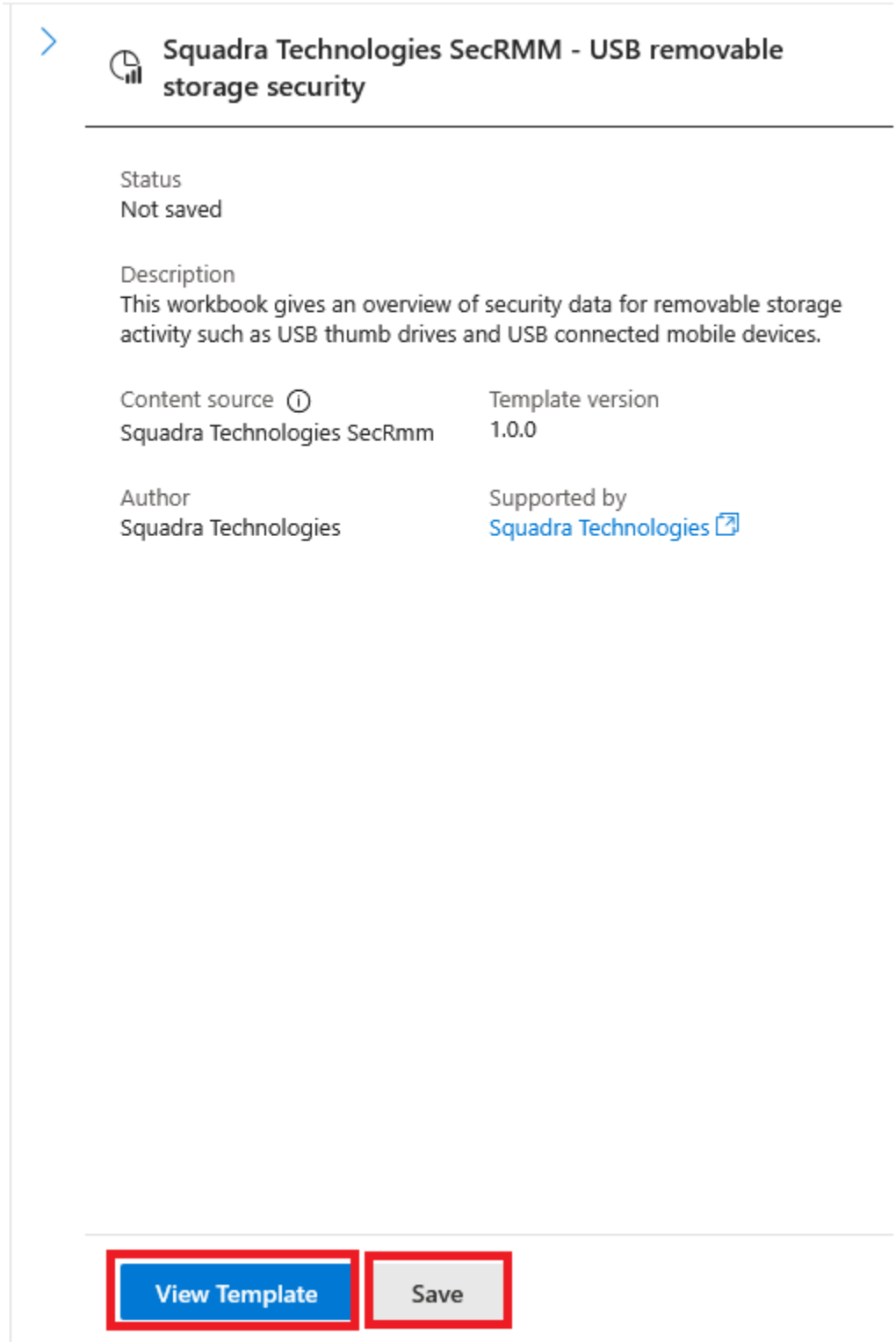
Click the ‘Templates’ tab as shown in the screenshot below.



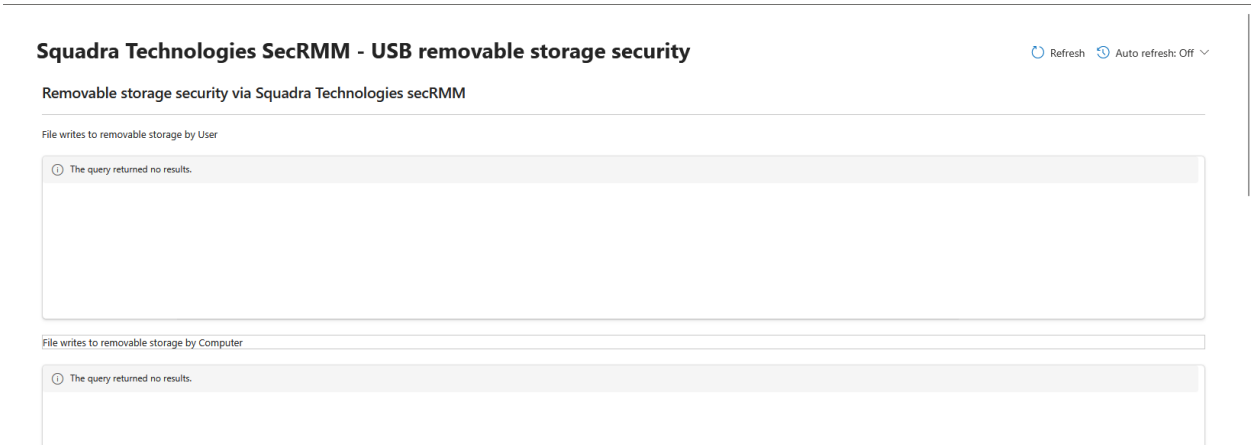
Click the ‘Squadra Technologies SecRMM - USB removable storage security’ as shown in the screenshot below.



At this point, you can either click ‘View Template’ or Save the workbook as shown in the screenshot below.



If you save the workbook, you can share it with others and make modifications to the workbook to suite your environment. Using 'View Template' can show you the default data that comes with the secRMM Data Connector as shown in the screenshot below.



Loading secRMM Azure Workbooks for tabular reporting

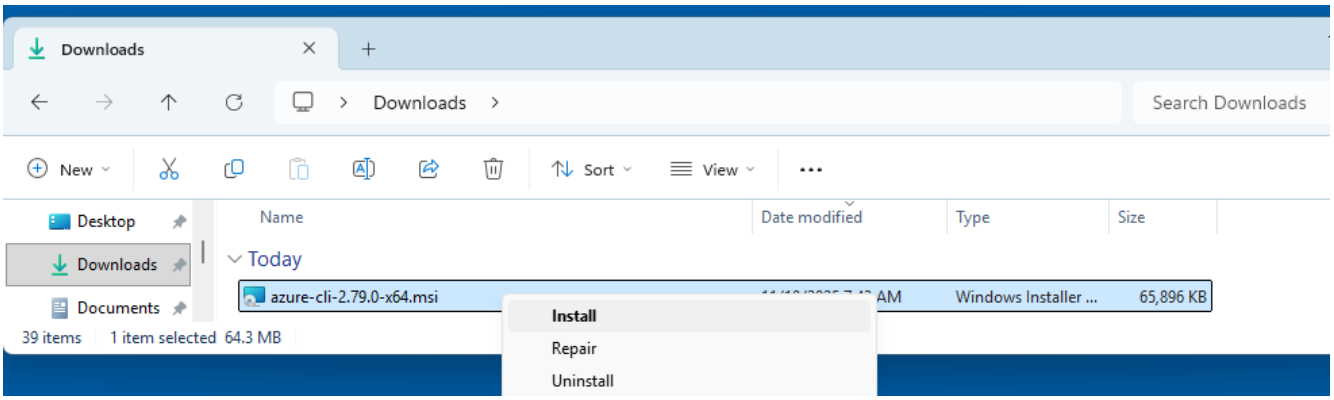
secRMM provides Azure Workbooks (reports) you can run to view the details of the secRMM data.

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.



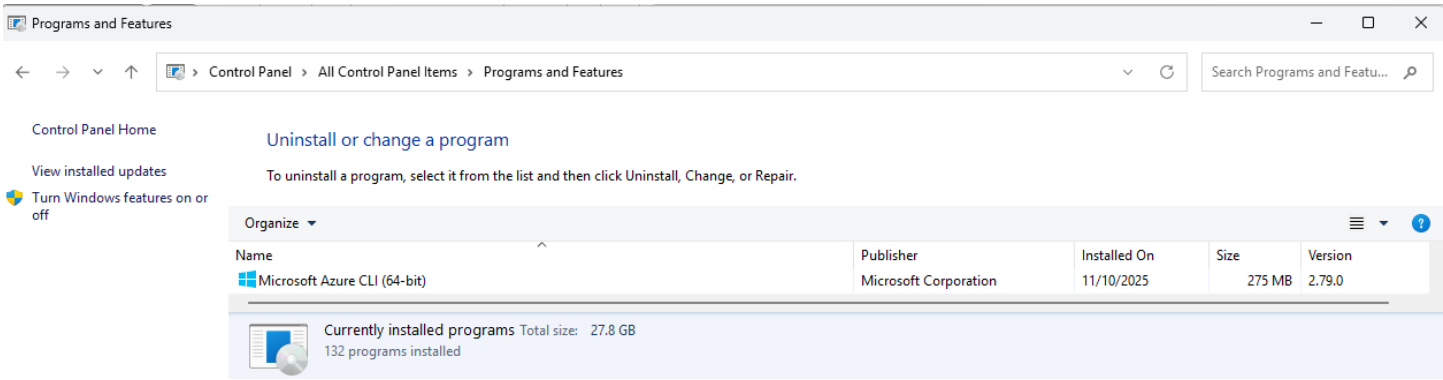
To verify your computer has the 'Azure CLI' version 2.x installed, open a CMD window and issue :

```
az --version
```

as shown in the screenshot below.

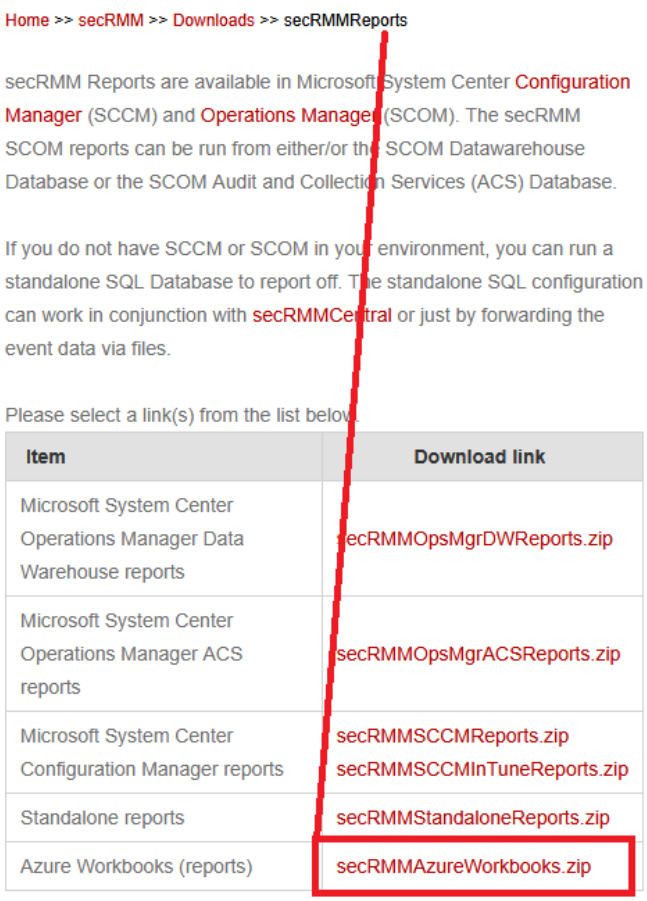
```
Administrator: cmd

C:\temp>where az
C:\Program Files\Microsoft SDKs\Azure\CLI2\wbin\az
C:\Program Files\Microsoft SDKs\Azure\CLI2\wbin\az.cmd

C:\temp>az --version
azure-cli                         2.79.0

core                              2.79.0
telemetry                          1.1.0

Extensions:
interactive                        0.5.3

Dependencies:
msal                            1.34.0b1
azure-mgmt-resource               23.3.0

Python location 'C:\Program Files\Microsoft SDKs\Azure\CLI2\python.exe'
Config directory 'C:\Users\Tony\.azure'
Extensions directory 'C:\Users\Tony\.azure\cliextensions'

Python (Windows) 3.13.9 (tags/v3.13.9:8183fa5, Oct 14 2025, 14:09:13) [MSC v.1944 64 bit (AMD64)]

Legal docs and information: aka.ms/AzureCliLegal


Your CLI is up-to-date.
```

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

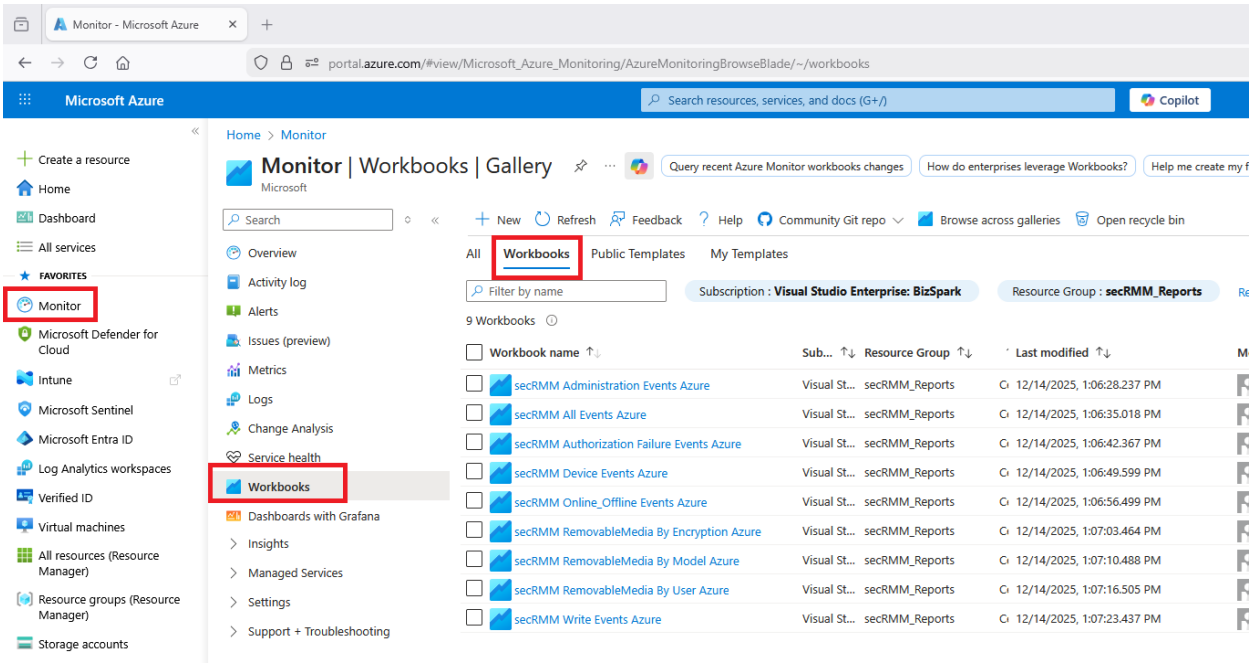
In the working directory where you extracted the zip file from above, go into PowerShell (by typing PowerShell in a CMD window) and then type:
.\ImportsecRMMAzureWorkbooks.ps1

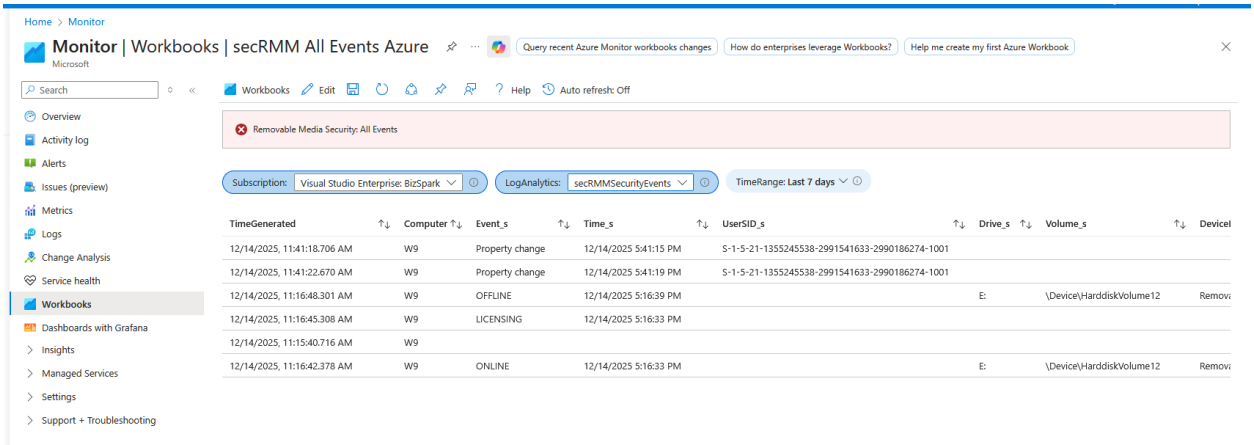
ImportsecRMMAzureWorkbooks.ps1 will prompt you to select:
1. An Azure Subscription (where the workbooks will be associated for billing)
2. An existing or new resource group (for example secRMM_Reports)
3. If you are creating a new resource group in step 2, you will be prompted to select a region to create 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 Microsoft Sentinel, we can tell Sentinel 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 Microsoft Sentinel instance. If you want help setting up your removable storage security strategy, please feel free to contact Squadra Technologies support (support@squadratechnologies.com).

Microsoft Sentinel Queries

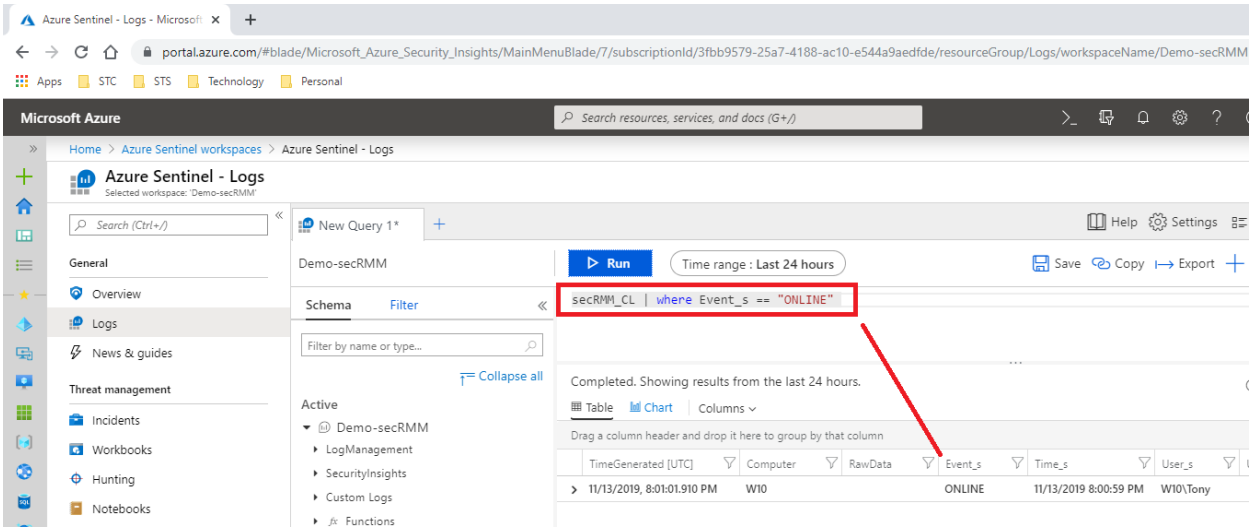
Azure uses a query language named "Keyword Query Language" (KQL). The samples below will show you KQL for the secRMM security events.

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"
```

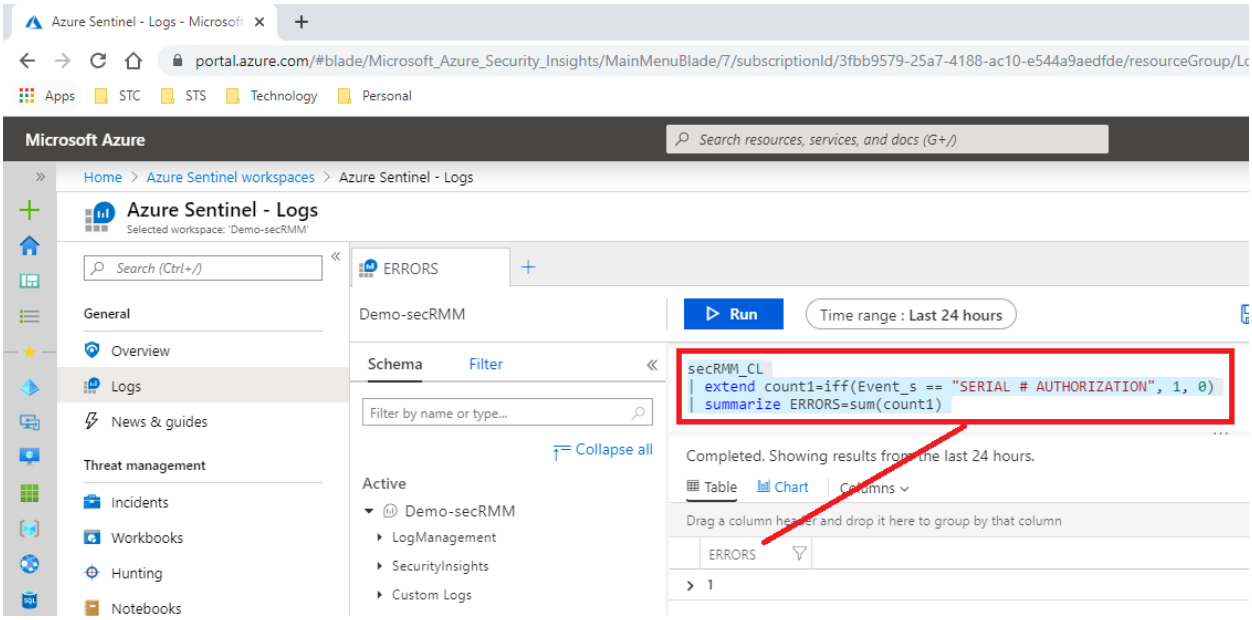


Sample query 2 – Count the number of failed write attempts events

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)
```

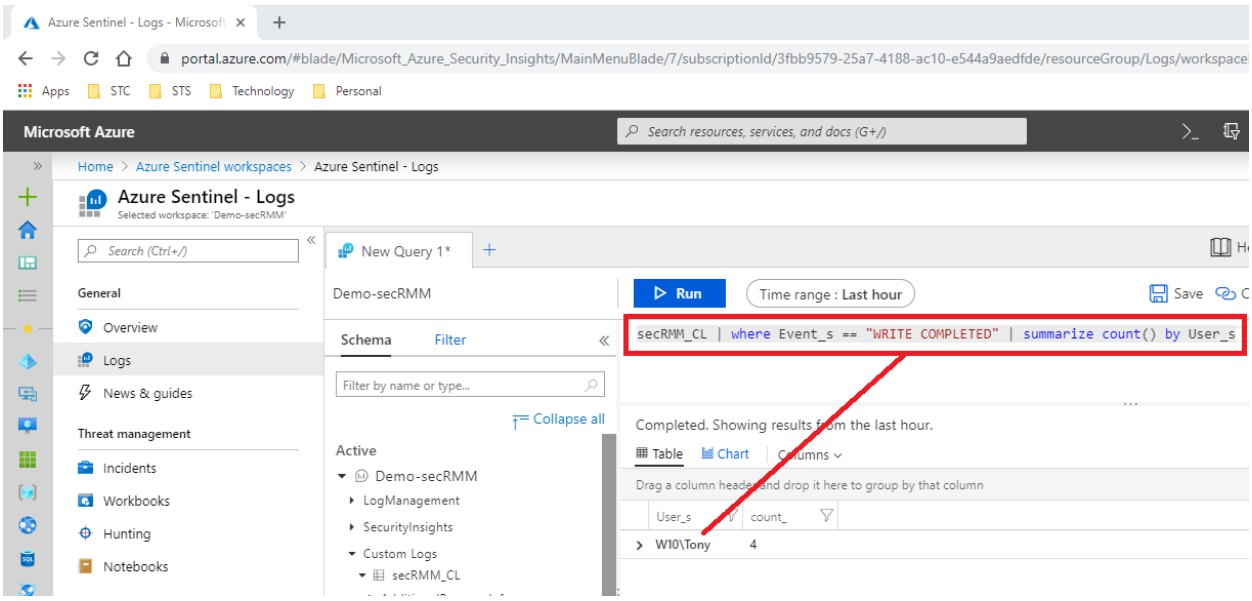
```
| summarize ERRORS=sum(count1)
```



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

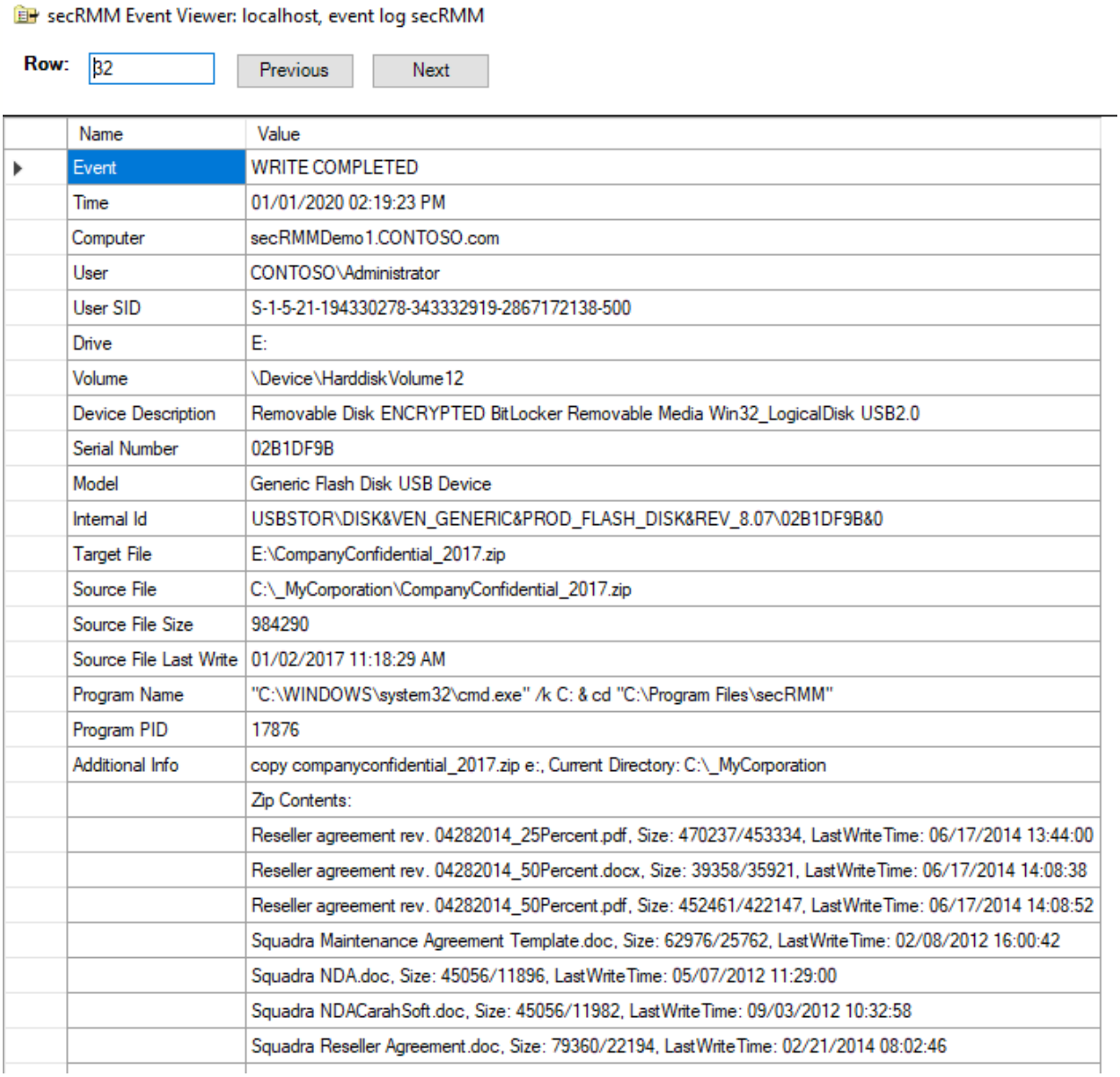
secRMM generates a security event for every file write attempt to a removable storage device that fails due to a security policy. If you want see which users and how many files each user is writing to removable storage, the KQL query is:

```
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

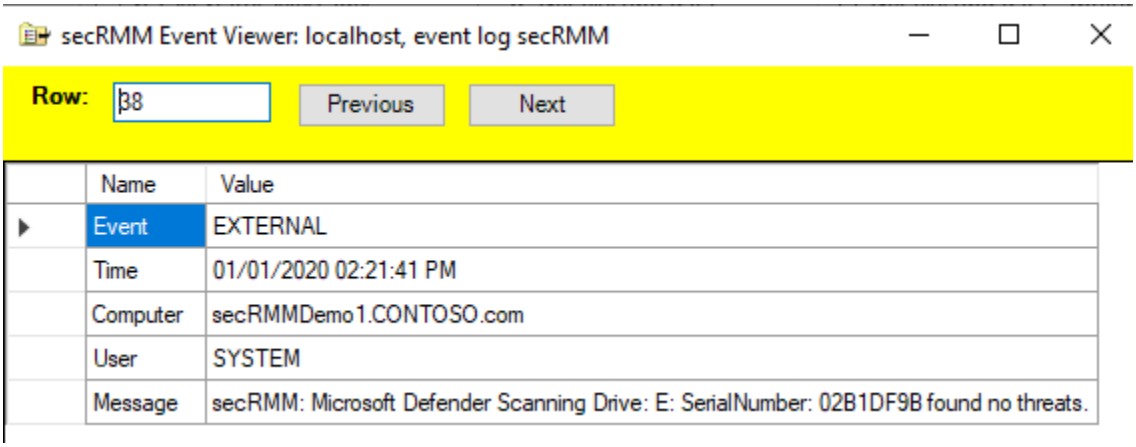
```
secRMM_CL | where DeviceDescription_s contains "ENCRYPTED BitLocker"
```



	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

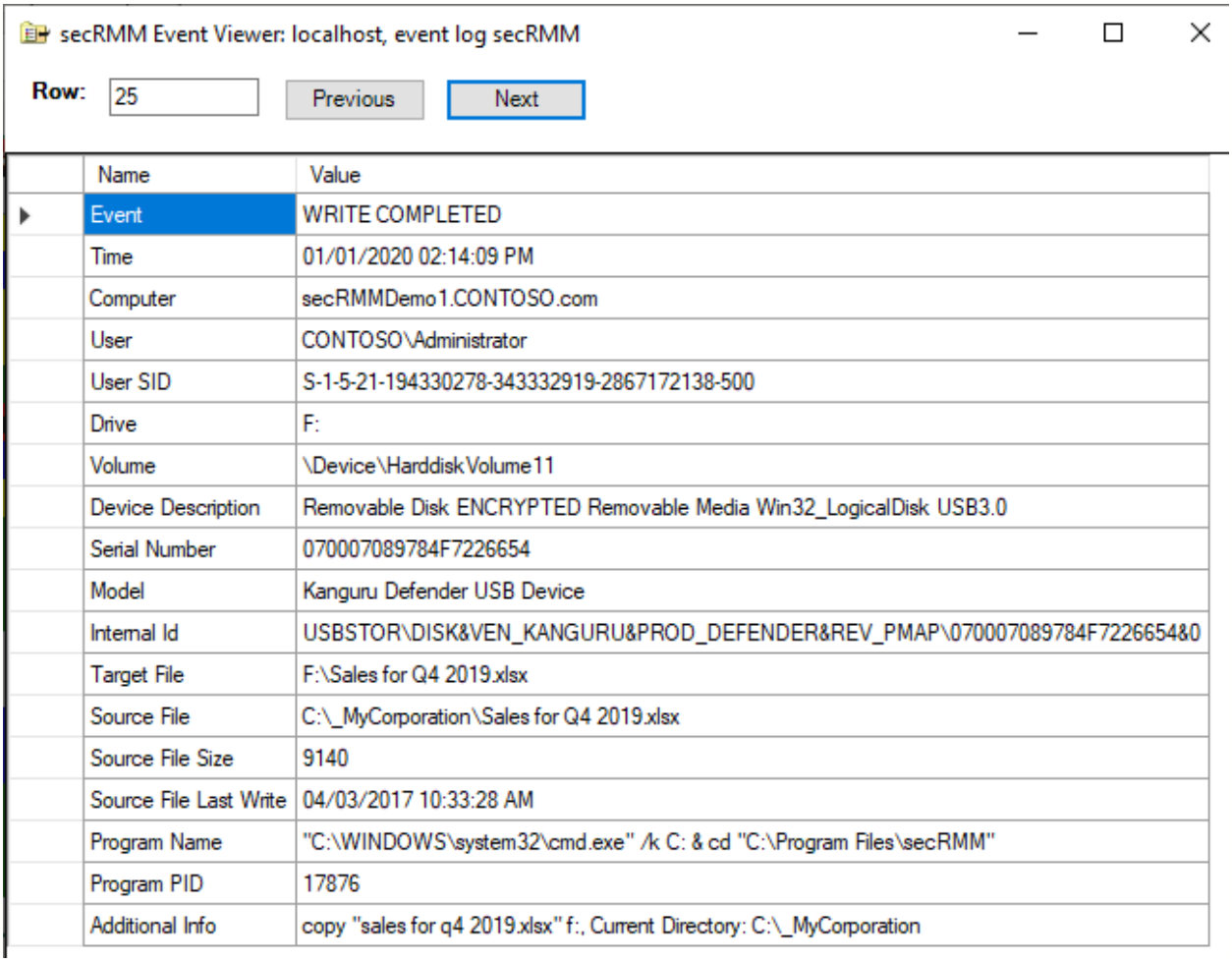
```
secRMM_CL | where ((Event_s == "EXTERNAL") and (Message contains "Microsoft Defender"))
```



	Name	Value
▶	Event	EXTERNAL
	Time	01/01/2020 02:21:41 PM
	Computer	secRMMDemo1.CONTOSO.com
	User	SYSTEM
	Message	secRMM: Microsoft Defender Scanning Drive: E: SerialNumber: 02B1DF9B found no threats.

Hardware Encrypted Device Activity

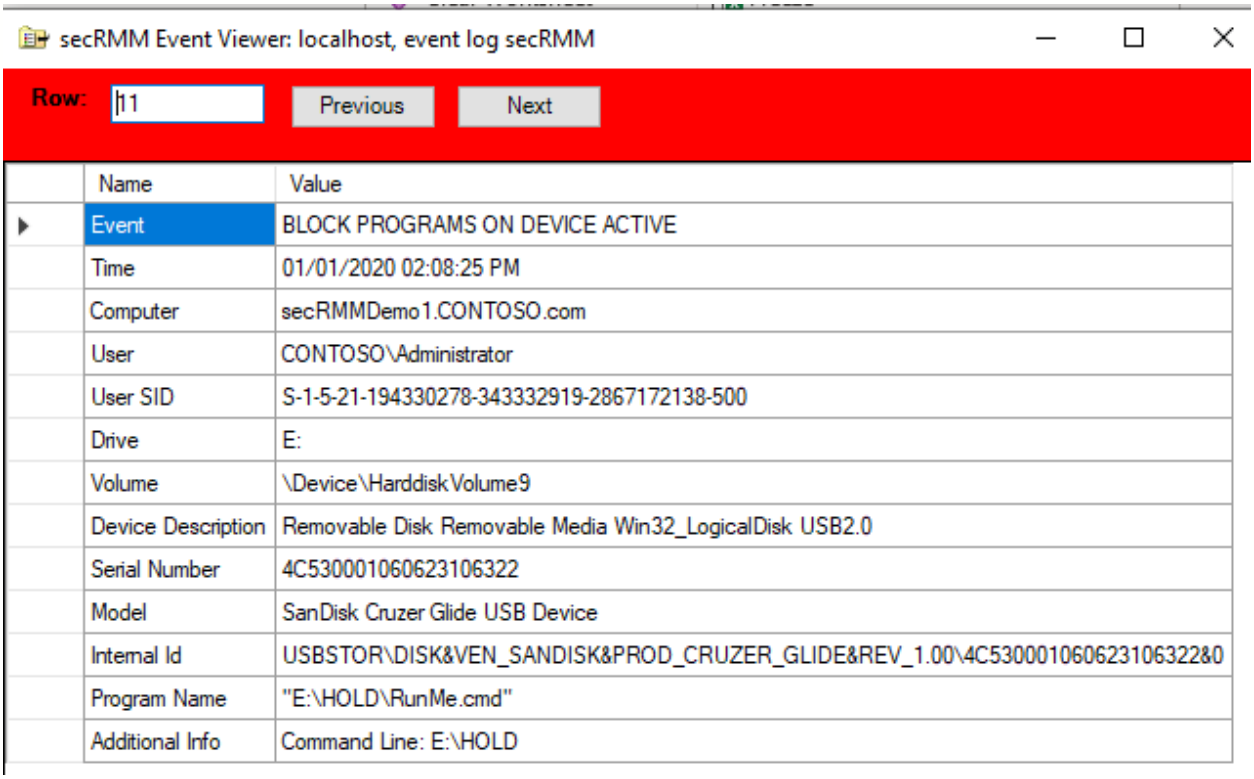
```
secRMM_CL | where DeviceDescription_s contains " ENCRYPTED Removable Media"
```



	Name	Value
▶	Event	WRITE COMPLETED
	Time	01/01/2020 02:14:09 PM
	Computer	secRMMDemo1.CONTOSO.com
	User	CONTOSO\Administrator
	User SID	S-1-5-21-194330278-343332919-2867172138-500
	Drive	F:
	Volume	\Device\HarddiskVolume11
	Device Description	Removable Disk ENCRYPTED Removable Media Win32_LogicalDisk USB3.0
	Serial Number	070007089784F7226654
	Model	Kanguru Defender USB Device
	Internal Id	USBSTOR\DISK&VEN_KANGURU&PROD_DEFENDER&REV_PMAP\070007089784F722665480
	Target File	F:\Sales for Q4 2019.xlsx
	Source File	C:_MyCorporation\Sales for Q4 2019.xlsx
	Source File Size	9140
	Source File Last Write	04/03/2017 10:33:28 AM
	Program Name	"C:\WINDOWS\system32\cmd.exe" /k C: & cd "C:\Program Files\secRMM"
	Program PID	17876
	Additional Info	copy "sales for q4 2019.xlsx" f:, Current Directory: C:_MyCorporation

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

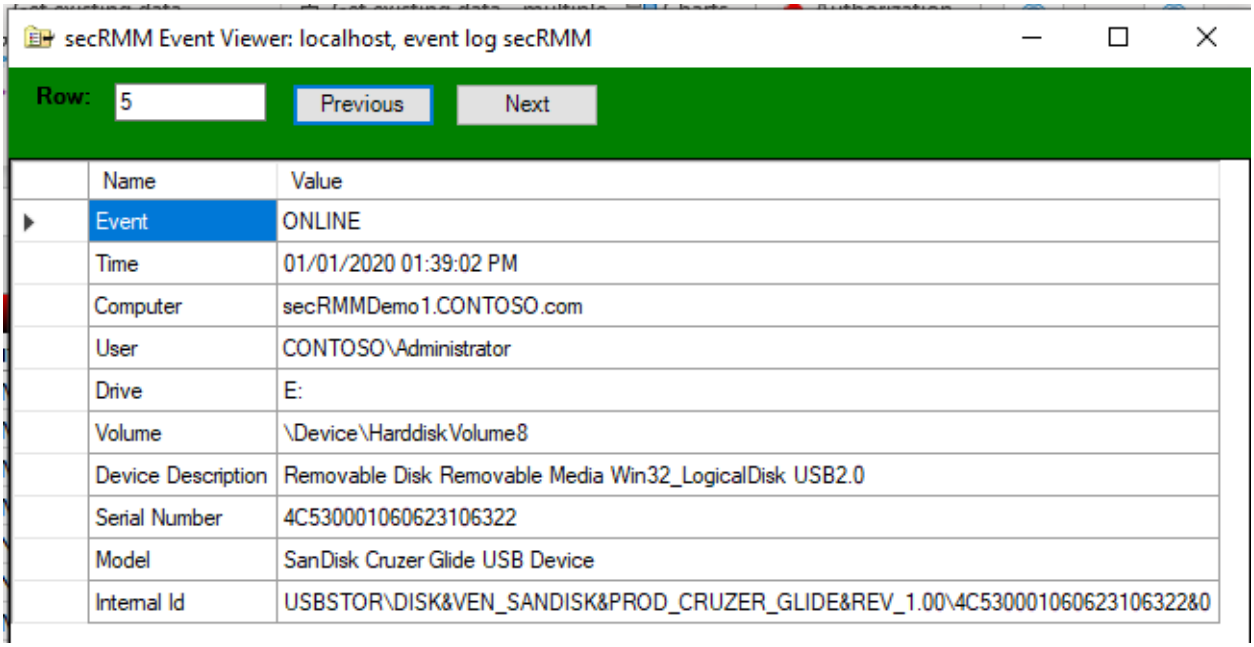
```
secRMM_CL | where ((Event_s == "BLOCK MACROS ON DEVICE ACTIVE") or (Event_s ==
"BLOCK PROGRAMS ON DEVICE ACTIVE")) | summarize count() by User_s
```



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"))
```

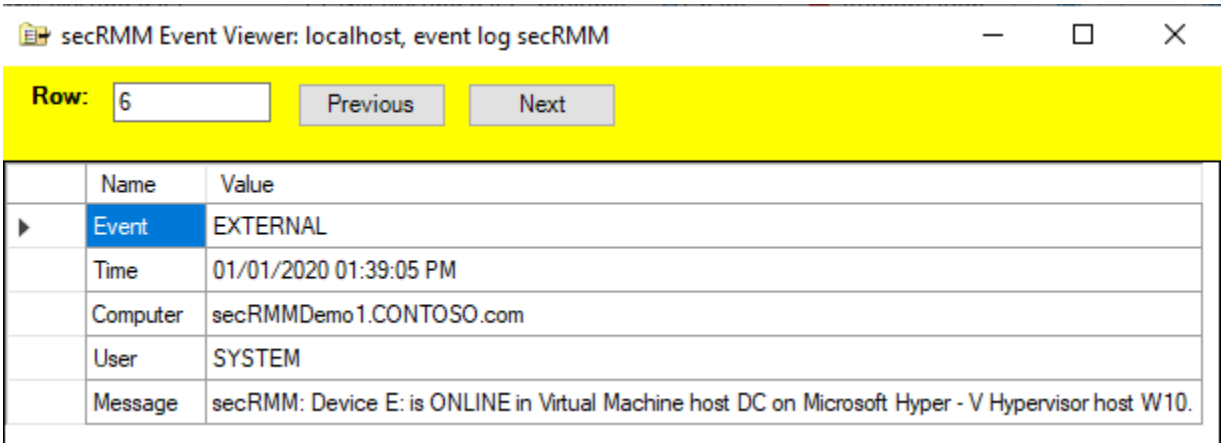


Name	Value
Event	ONLINE
Time	01/01/2020 01:39:02 PM
Computer	secRMMDemo1.CONTOSO.com
User	CONTOSO\Administrator
Drive	E:
Volume	\Device\HarddiskVolume8
Device Description	Removable Disk Removable Media Win32_LogicalDisk USB2.0
Serial Number	4C530001060623106322
Model	SanDisk Cruzer Glide USB Device
Internal Id	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_GLIDE&REV_1.00\4C530001060623106322&0

Removable storage devices that are mounted into a Virtual Machine

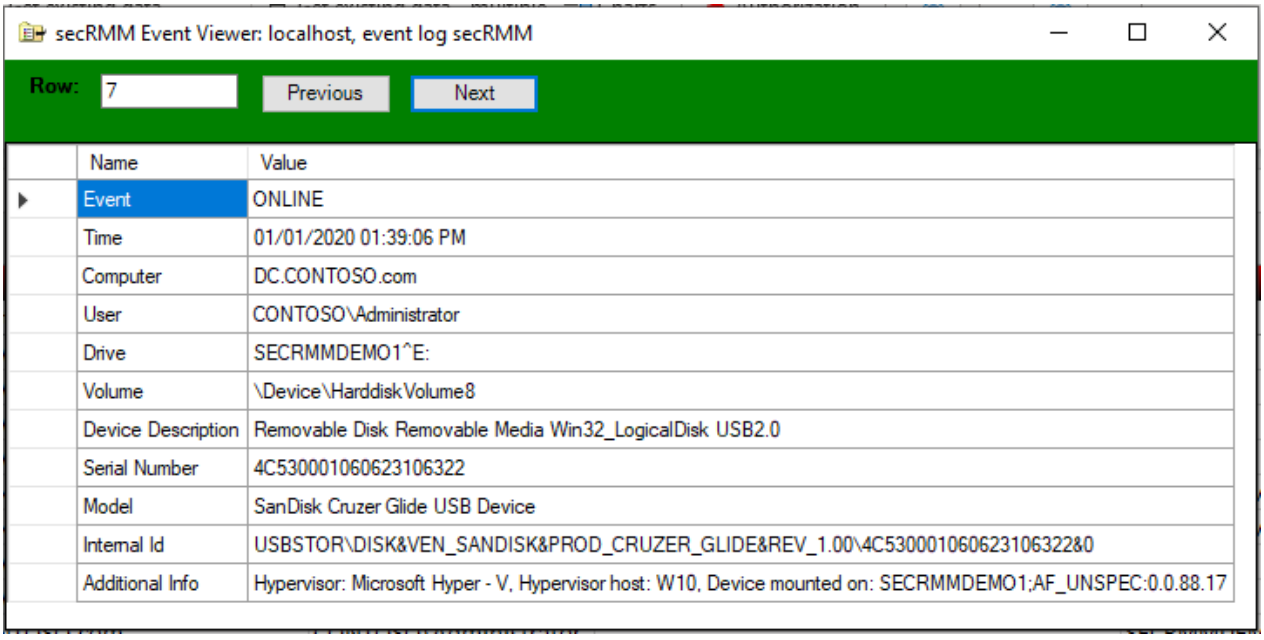
Event on the physical machine

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



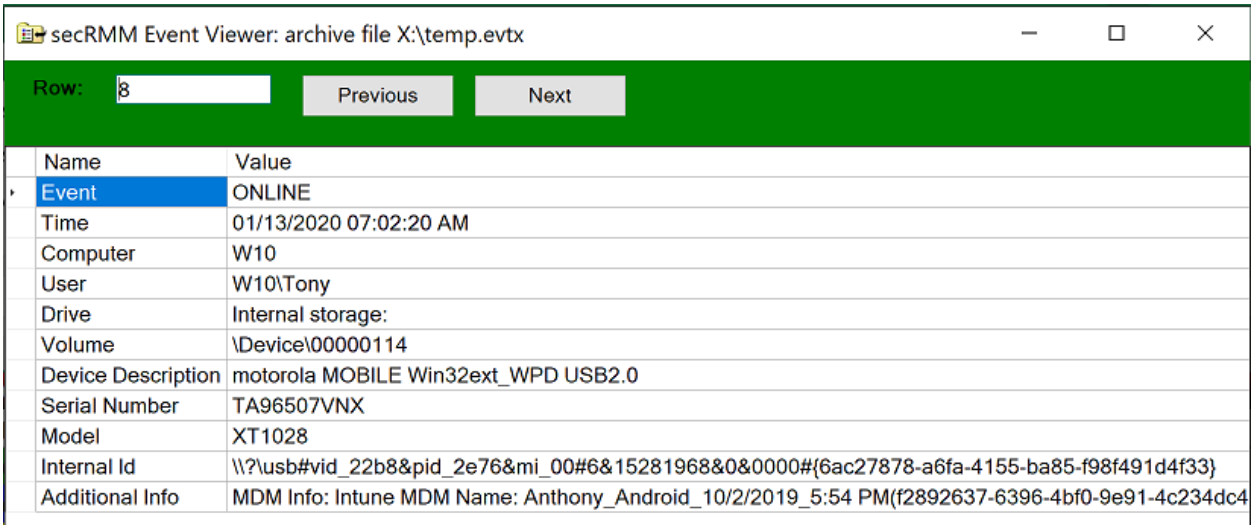
Event on the virtual machine

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



Show mobile devices that are being USB mounted

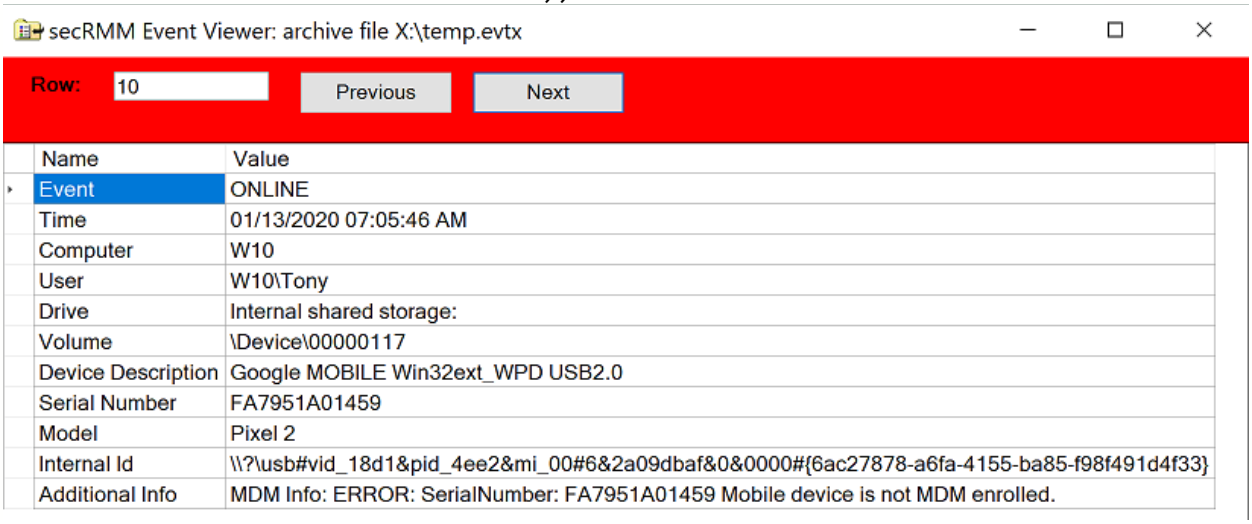
```
secRMM_CL | where ((Event_s == "ONLINE") and (DeviceDescription_s contains
"MOBILE"))
```



Name	Value
Event	ONLINE
Time	01/13/2020 07:02:20 AM
Computer	W10
User	W10\Tony
Drive	Internal storage:
Volume	\Device\00000114
Device Description	motorola MOBILE Win32ext_WPD USB2.0
Serial Number	TA96507VNX
Model	XT1028
Internal Id	\\?\usb#vid_22b8&pid_2e76&mi_00#6&15281968&0&0000#{6ac27878-a6fa-4155-ba85-f98f491d4f33}
Additional Info	MDM Info: Intune MDM Name: Anthony_Android_10/2/2019_5:54 PM(f2892637-6396-4bf0-9e91-4c234dc4

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

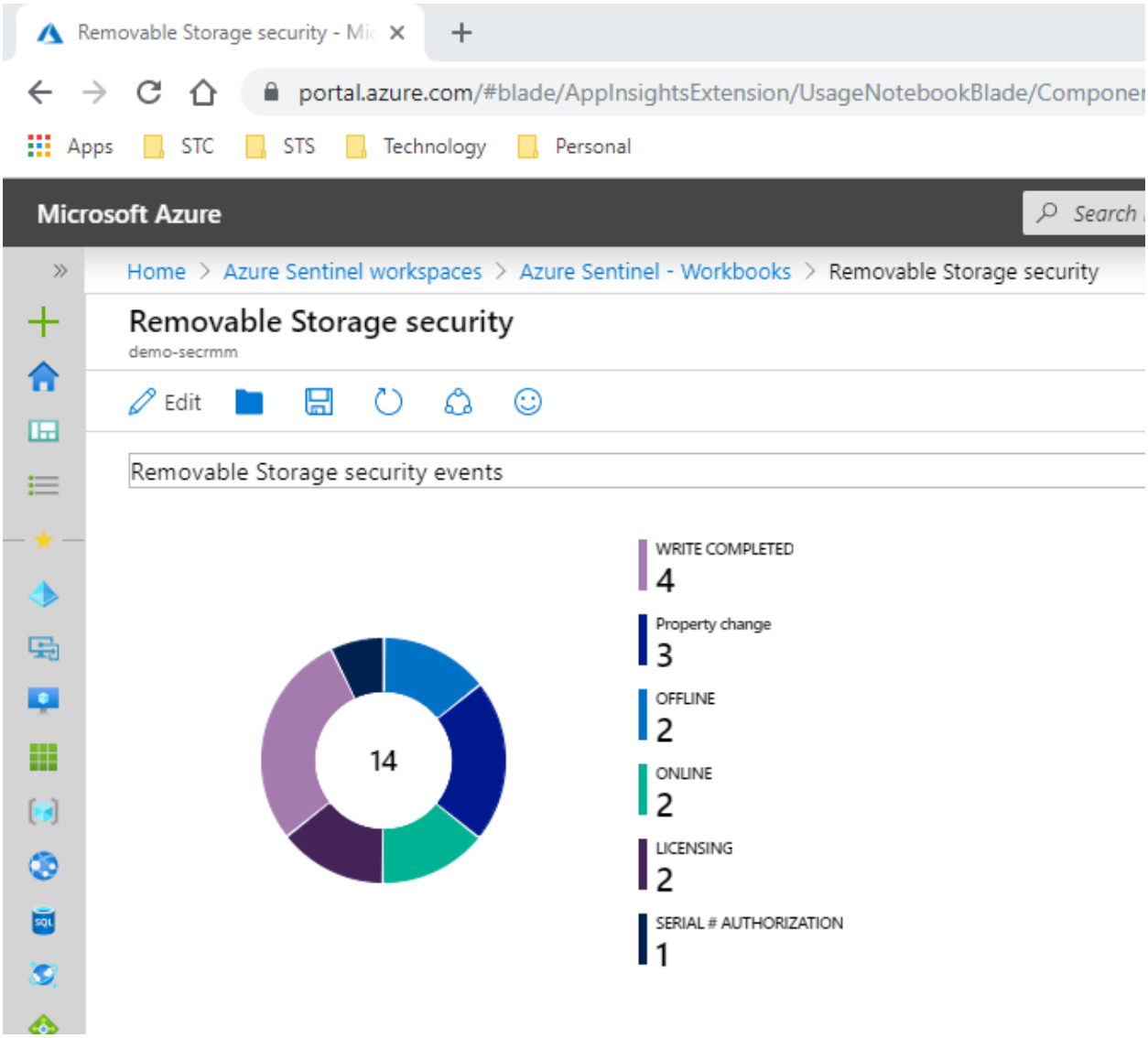
```
secRMM_CL | where ((Event_s == "ONLINE") and (AdditionalProgramInfo_s contains
"Mobile device is not MDM enrolled"))
```



Name	Value
Event	ONLINE
Time	01/13/2020 07:05:46 AM
Computer	W10
User	W10\Tony
Drive	Internal shared storage:
Volume	\Device\00000117
Device Description	Google MOBILE Win32ext_WPD USB2.0
Serial Number	FA7951A01459
Model	Pixel 2
Internal Id	\\?\usb#vid_18d1&pid_4ee2&mi_00#6&2a09dbaf&0&0000#{6ac27878-a6fa-4155-ba85-f98f491d4f33}
Additional Info	MDM Info: ERROR: SerialNumber: FA7951A01459 Mobile device is not MDM enrolled.

Microsoft Sentinel Workbook

You can create an “Microsoft Sentinel Workbook” to see graphs and charts of the removable storage security events.

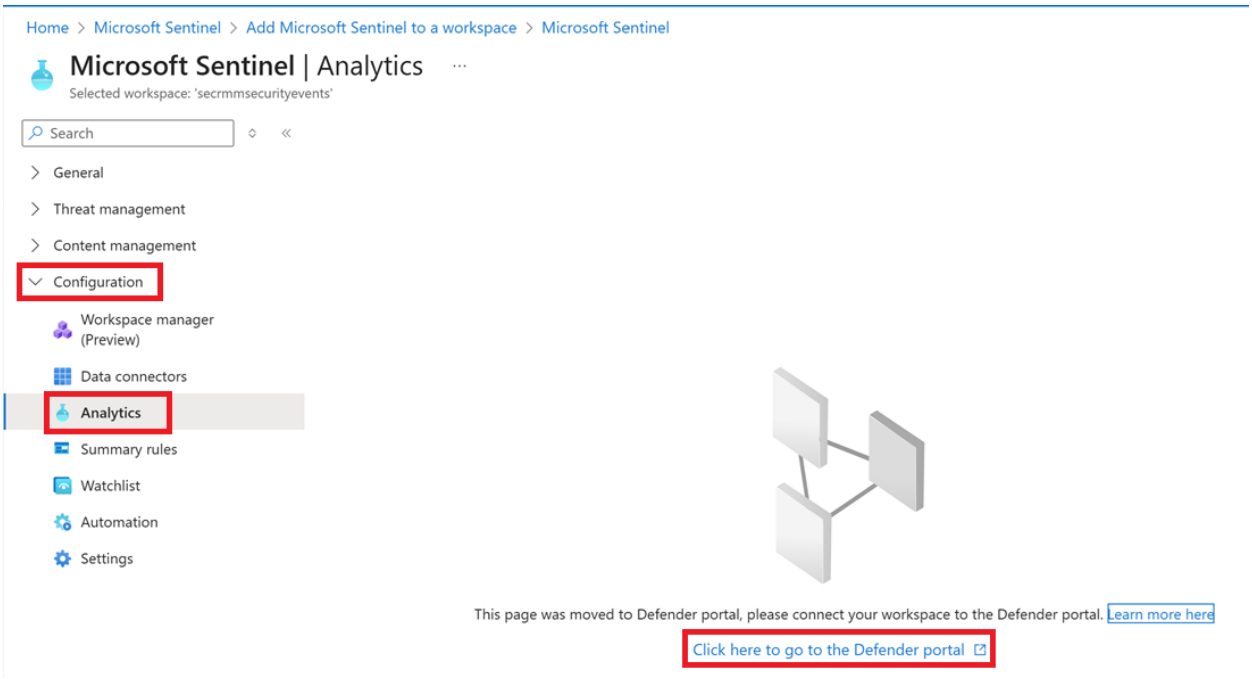


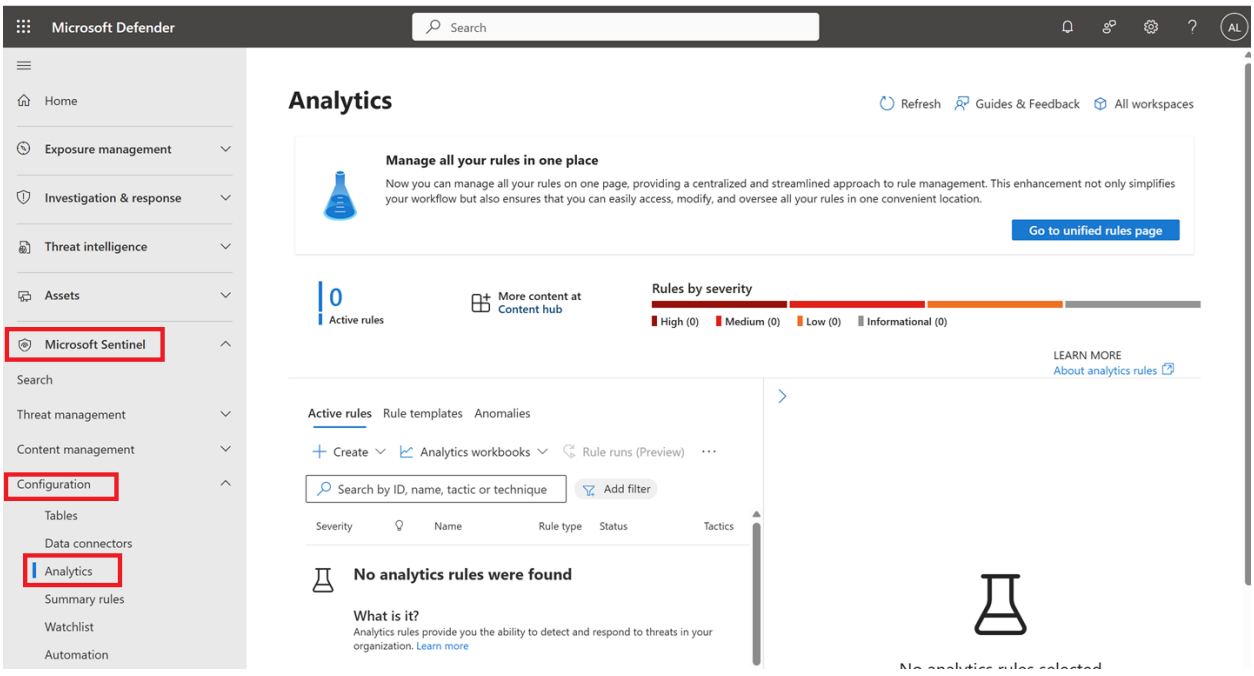
There is currently no method to import a workbook into you Microsoft Sentinel instance. When a method becomes available from Microsoft, we will update the process for you. For now, please download the json file (which is the Sentinel workbook) on github at: https://github.com/anthonylamark/secRMMAzureSentinel

Microsoft Sentinel Analytics

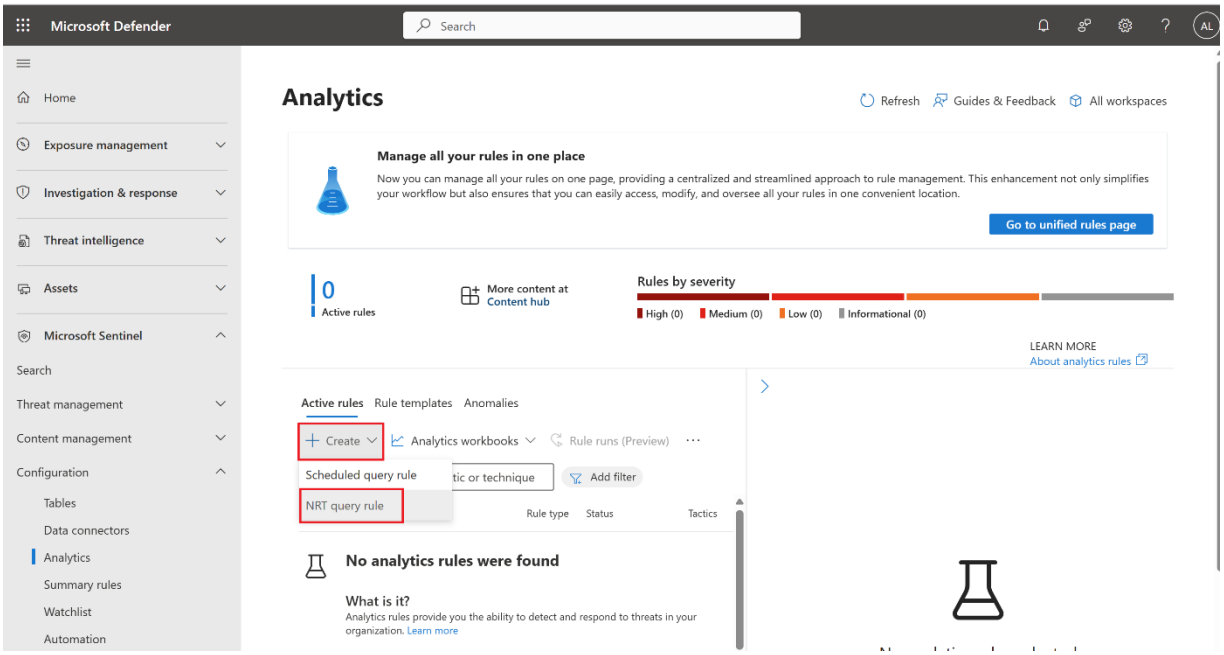
This section will use "Microsoft Sentinel Analytics" to make your "Microsoft Sentinel Dashboard" show you when removable storage devices are getting USB mounted (i.e. plugged in, i.e. a secRMM ONLINE event) to the Windows computers in your environment. You may want to integrate other removable storage security events into your Microsoft Sentinel Dashboard. The process for each will be similar to ONLINE event we show below.

Click the "**Analytics**" link (as shown in the screenshot below). Note that the Microsoft Sentinel Analytics has been moved into the Defender portal.

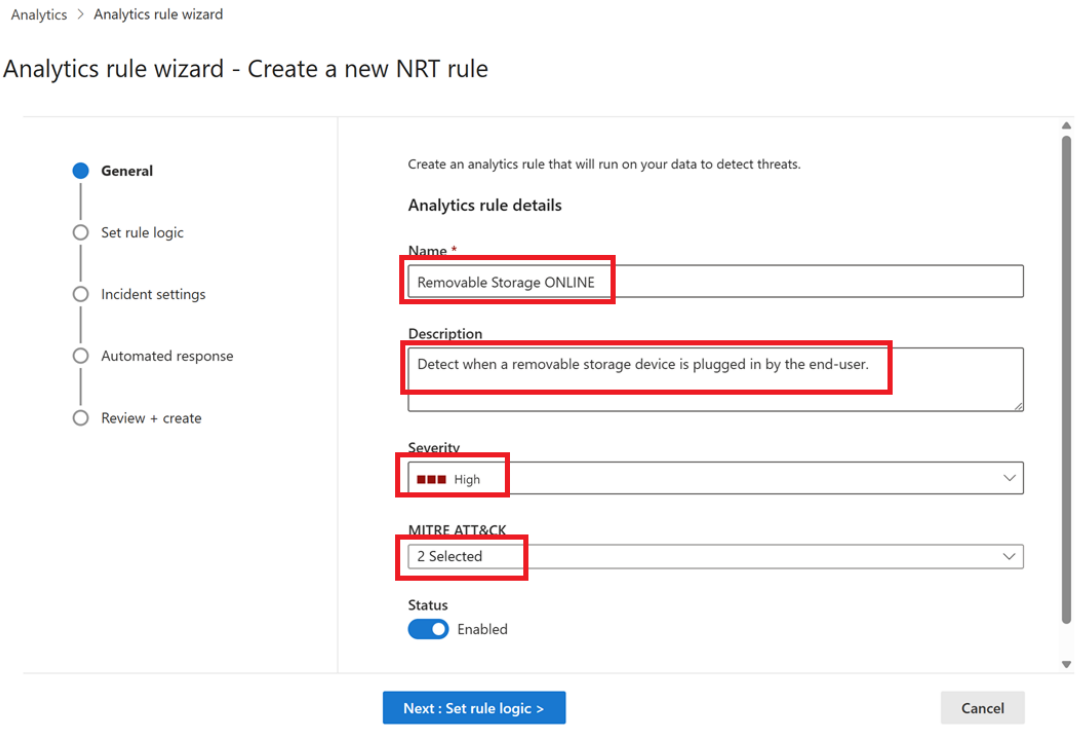


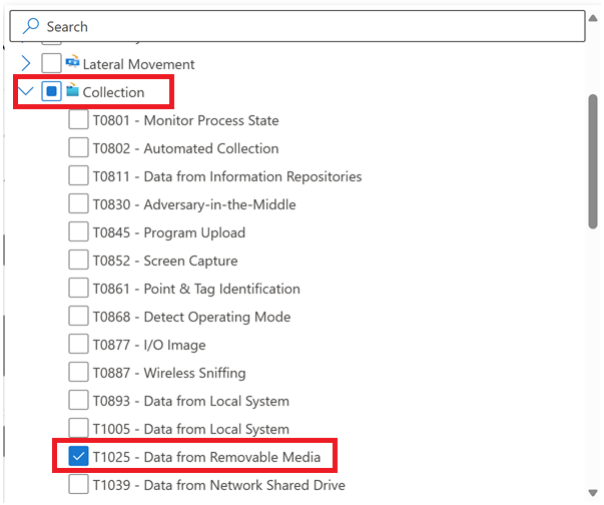


Click the "**Create**" link and then select the "**NRT query rule**" (as shown in the screenshot below).



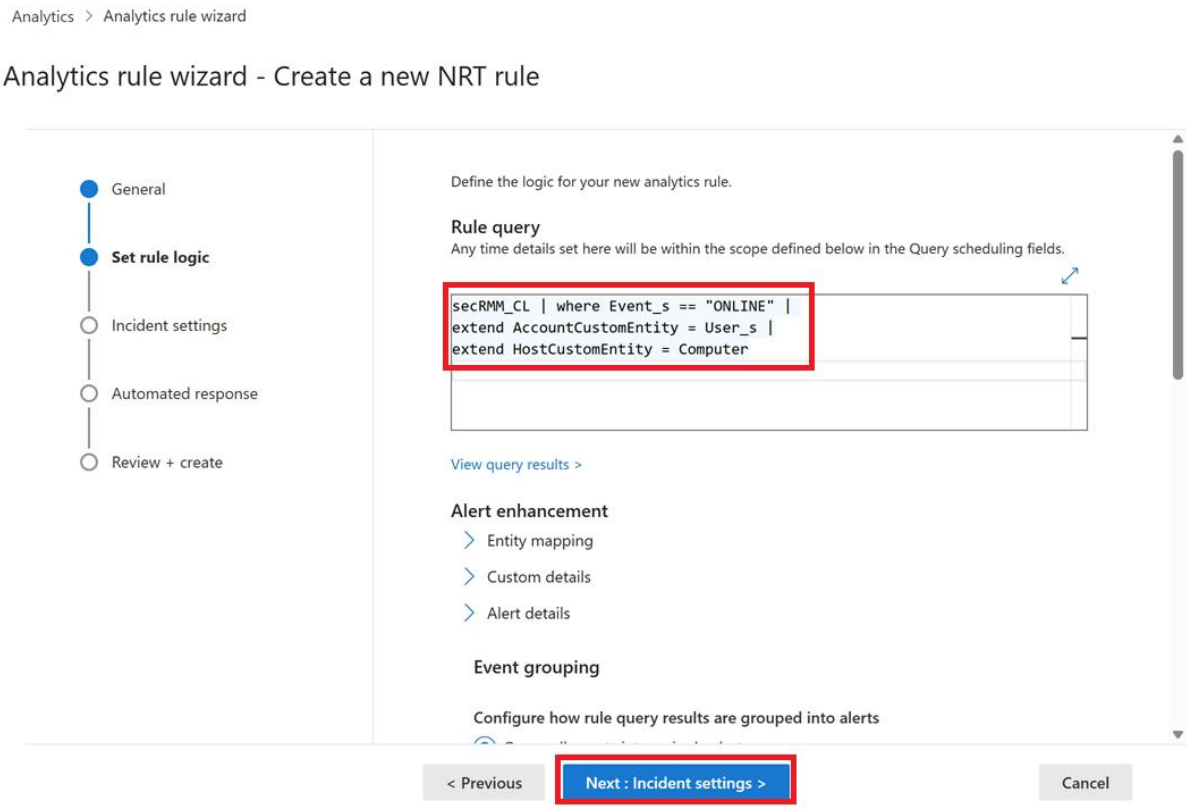
Fill in the form and then click the “Next : Set rule logic” button (as shown in the first screenshot below). For the ‘MITRE ATTACK’, check Collection and then ‘Data from Removable Media’ (as shown in the second screenshot below).



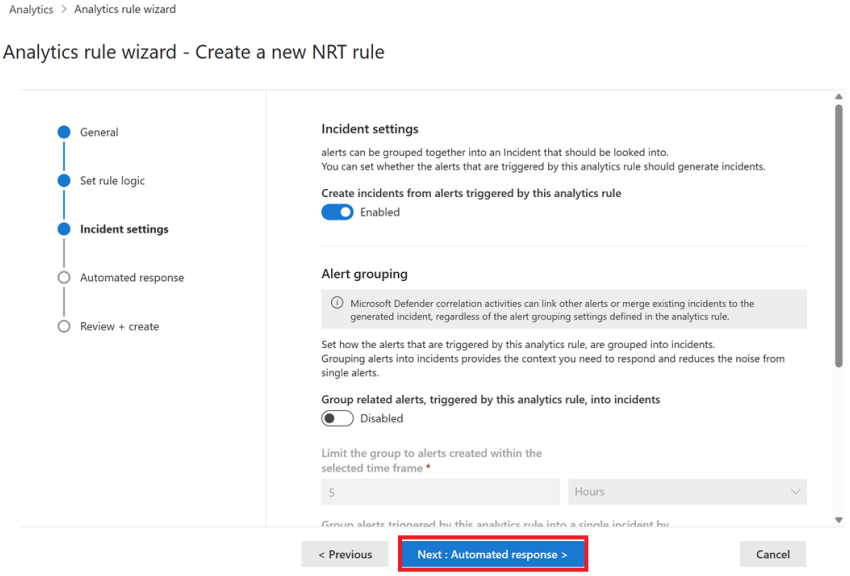


Put the following query into the “Rule query” text field in the next form and then click the “Next : Incident settings” button (as shown in the screenshot below).

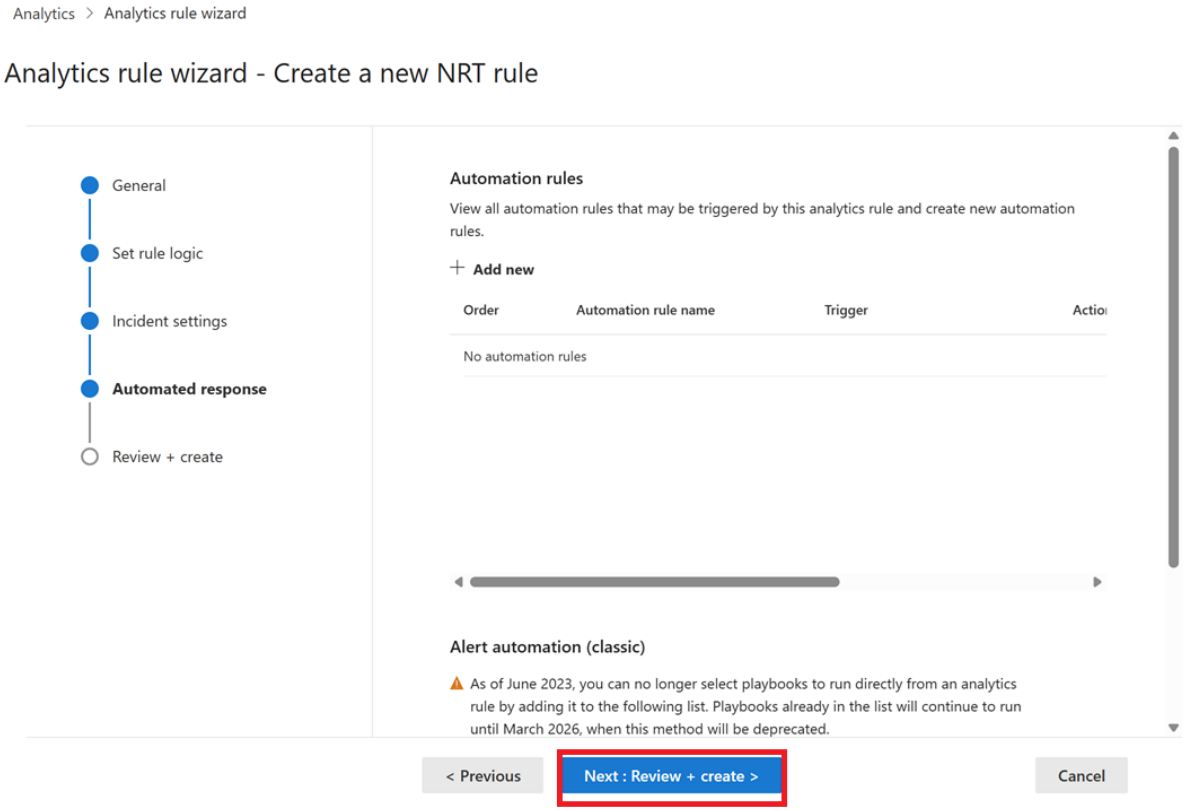
```
secRMM_CL | where Event_s == "ONLINE"|
extend AccountCustomEntity = User_s |
extend HostCustomEntity = Computer
```



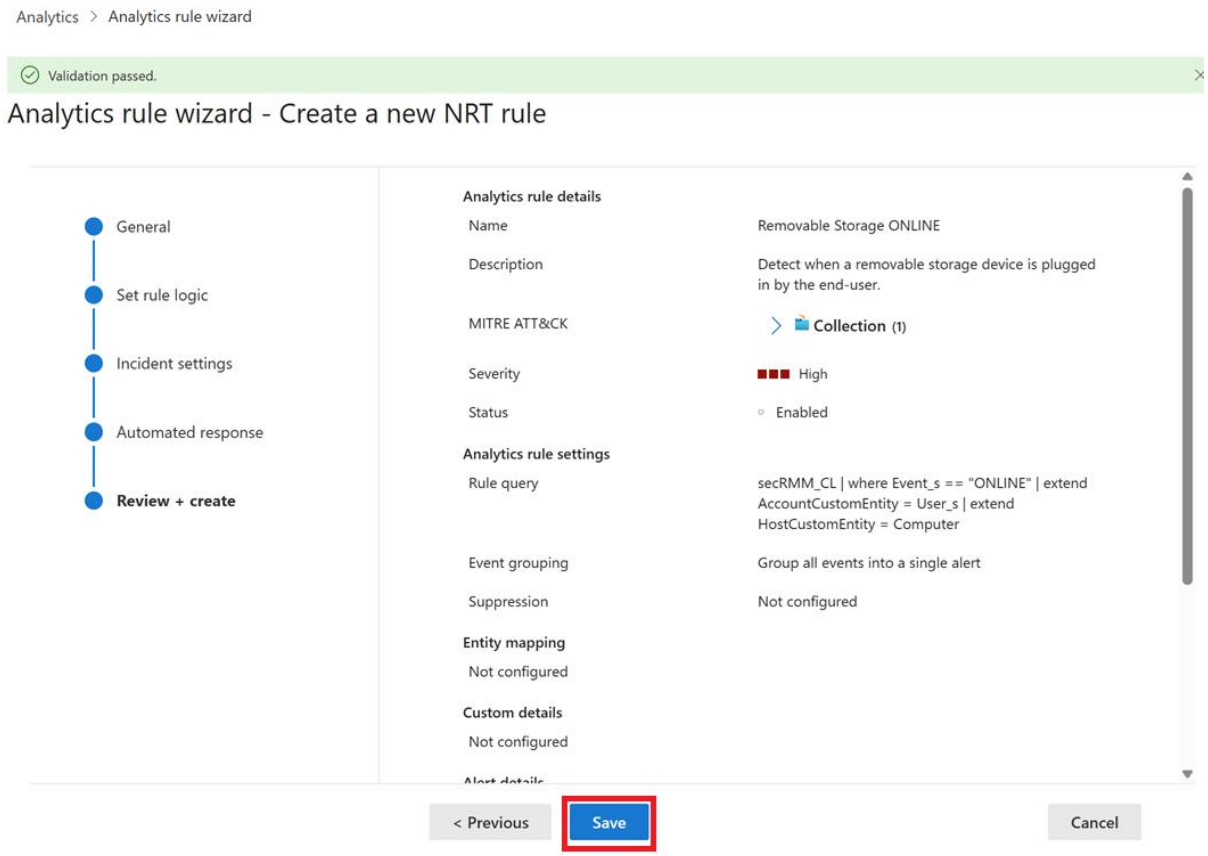
Click the “Next : Automated response” button (as shown in the screenshot below).



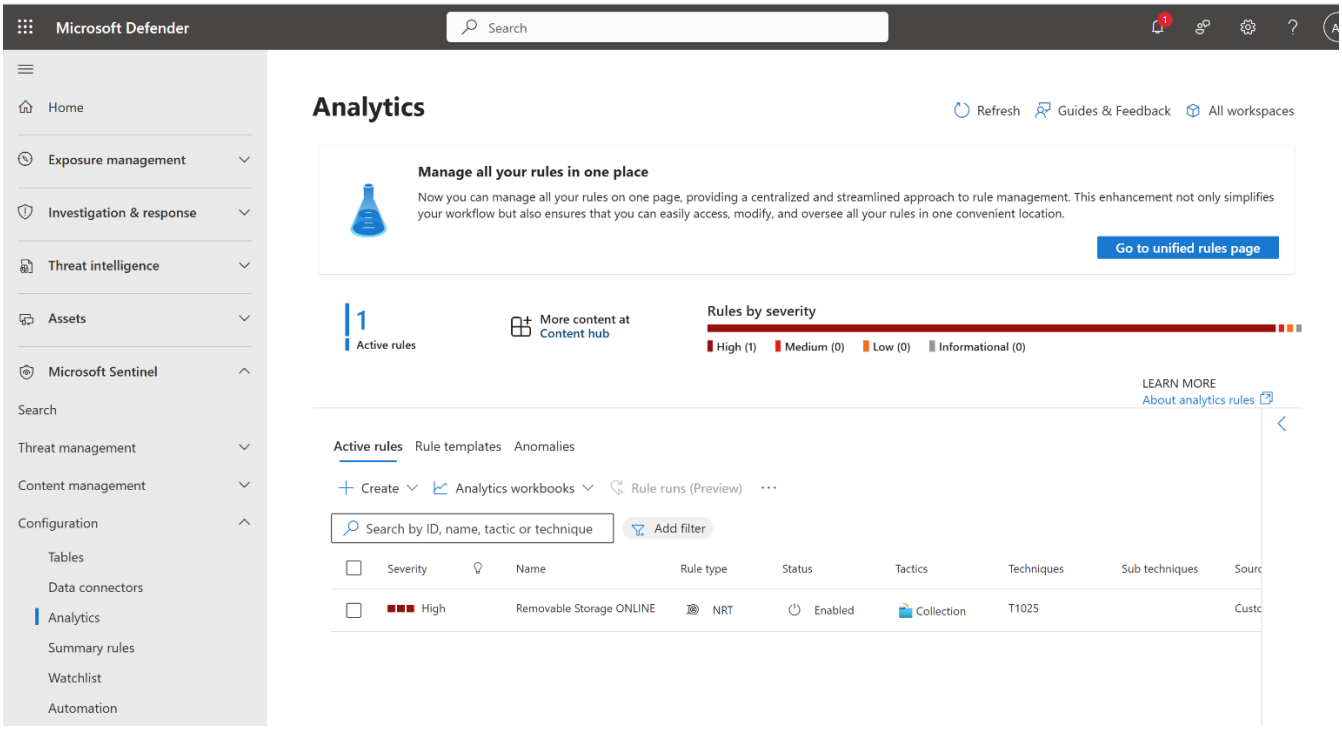
Once you have the form filled out, click the “**Review and Create**” link (as shown in the screenshot below).



Now click the “Create” button (as shown in the screenshot below).

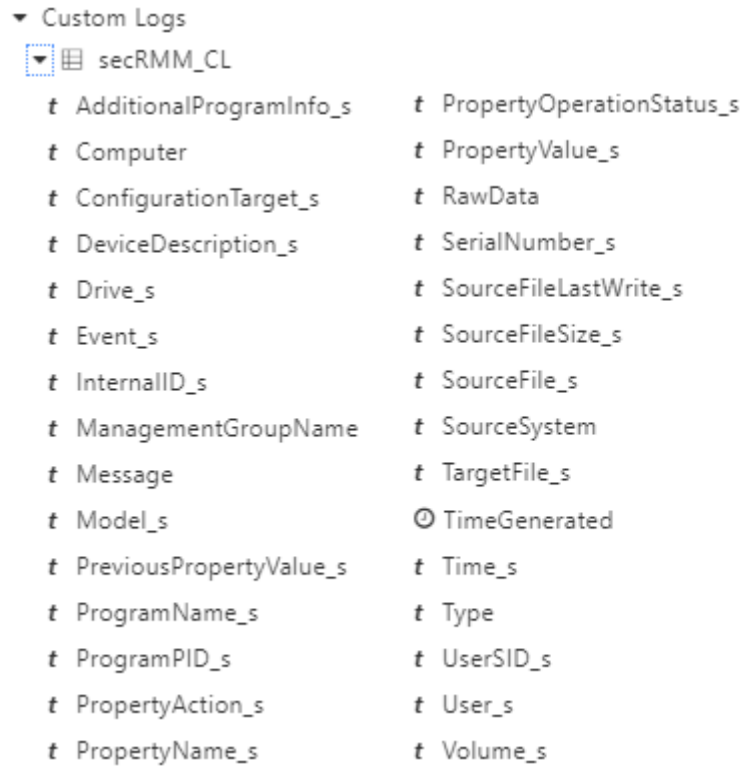


Your rule will now show up in the list (as shown in the screenshot below).



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, Missouri 64734
USA
Web site https://www.squadratechnologies.com/