



Security Removable Media Manager
connector to

Defender for Cloud

Version 9.11.27.0
(April 2024)

Protect your valuable data



Microsoft Defender for Cloud

secRMM Defender for Cloud Administrator 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
7575 West Washington Ave
Suite 127-252
Las Vegas, NV 89128 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

secRMM Defender for Cloud Administrator Guide

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’ | 10 |
| CONNECT “AZURE LOG WORKSPACE FOR secRMM” TO MICROSOFT DEFENDER FOR CLOUD | 19 |
| CONFIGURE secRMM TO SEND EVENTS TO “AZURE LOG WORKSPACE FOR secRMM” | 20 |
| USAGE | 22 |
| AZURE DEFENDER FOR CLOUD QUERIES | 23 |
| <i>Sample query 1 – ONLINE events.....</i> | <i>23</i> |
| <i>Sample query 2 – Count the number of failed write attempts events.....</i> | <i>23</i> |
| <i>Sample query 3 – Which users are writing files to removable storage devices</i> | <i>24</i> |
| <i>Sample query 4 – Which users attempted writing files to removable storage devices but failed.....</i> | <i>25</i> |
| <i>More sample queries.....</i> | <i>25</i> |
| Microsoft BitLocker Activity for removable storage devices | 25 |
| Microsoft Windows Defender Activity for removable storage devices | 26 |
| Hardware Encrypted Device Activity | 27 |
| Users who have tried to execute macros or programs from a removable storage device | 27 |
| Removable storage devices that are not encrypted (hardware or software) | 28 |
| Removable storage devices that are mounted into a Virtual Machine | 29 |
| Event on the physical machine | 29 |
| Event on the virtual machine..... | 29 |
| Show mobile devices that are being USB mounted..... | 30 |
| Show mobile devices that are being USB mounted but are not MDM (Microsoft Intune) enrolled | 30 |
| AZURE LOG ANALYTICS secRMM SCHEMA | 31 |
| <i>Descriptions.....</i> | <i>31</i> |
| CONTACTING SQUADRA TECHNOLOGIES SUPPORT | 32 |
| ABOUT SQUADRA TECHNOLOGIES, LLC..... | 33 |

secRMM Defender for Cloud Administrator Guide

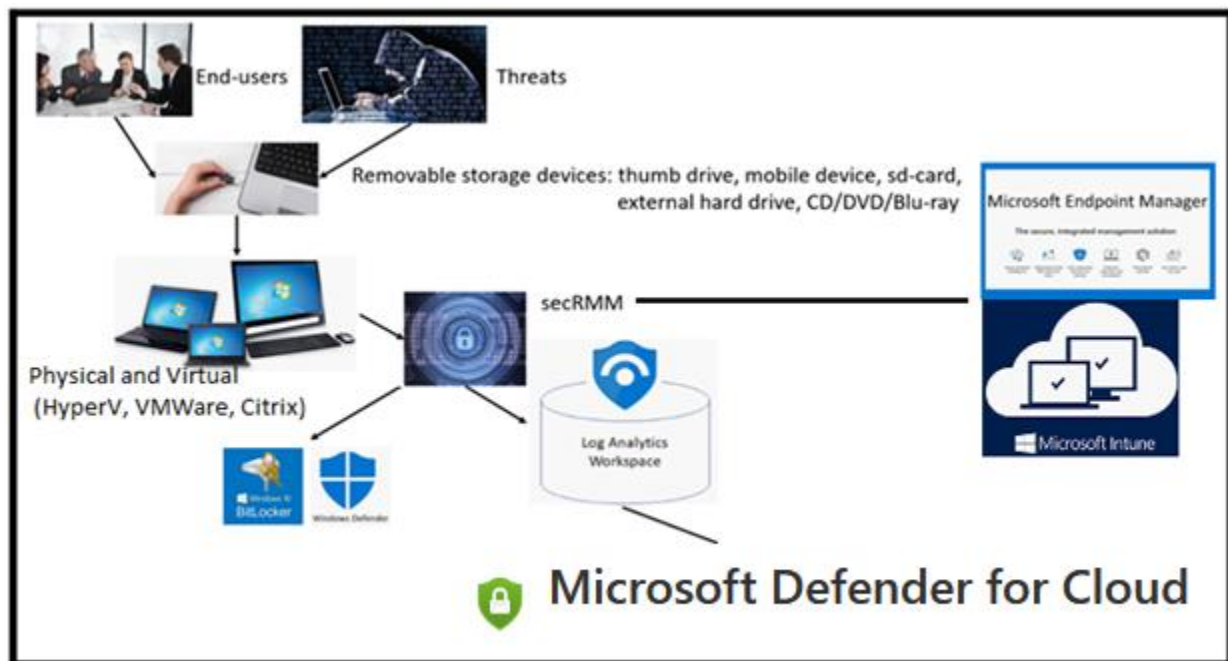
Introduction

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.

secRMM Defender for Cloud Administrator Guide

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:

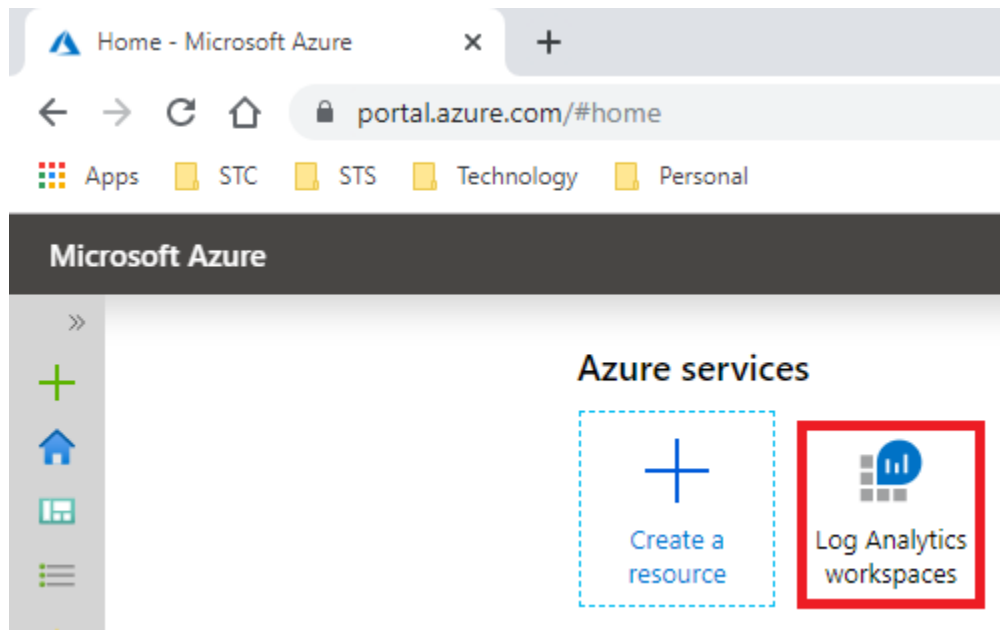
<http://www.squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx>, under the “secRMM Installation” section (as shown in the screenshot below).



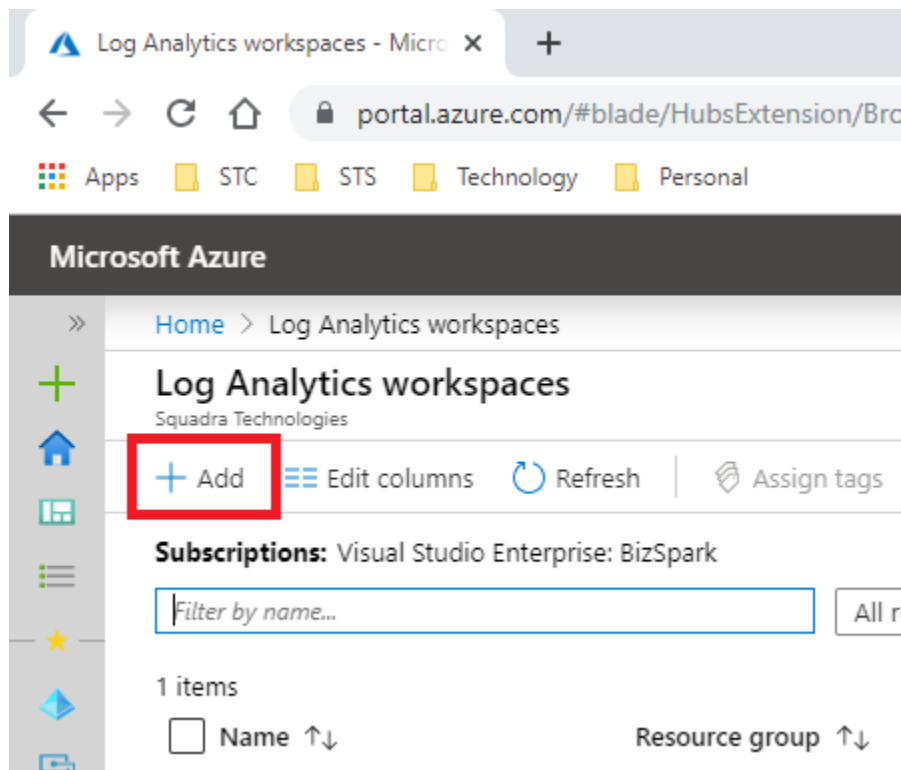
Create “Azure Log Workspace for secRMM”

Within your Azure portal, go to “Log Analytics workspaces” (as shown in the screenshot below).

secRMM Defender for Cloud Administrator Guide



Within your Azure “Log Analytics workspaces”, click the Add link (as shown in the screenshot below).



Fill out the form (as shown in the screenshot below).
Note that the values you specify here will be different based on your Azure environment.

secRMM Defender for Cloud Administrator Guide

Log Analytics workspace - Micros x +

portal.azure.com/#create/Microsoft.LogAnalyt

Apps STC STS Technology Personal

Microsoft Azure

Home > Log Analytics workspaces > Log Analytics workspace

Log Analytics workspace □ ×
Create new or link existing workspace

☒ Create New ☐ Link Existing

Log Analytics Workspace * ⓘ
secRMMSecurityEvents ✓

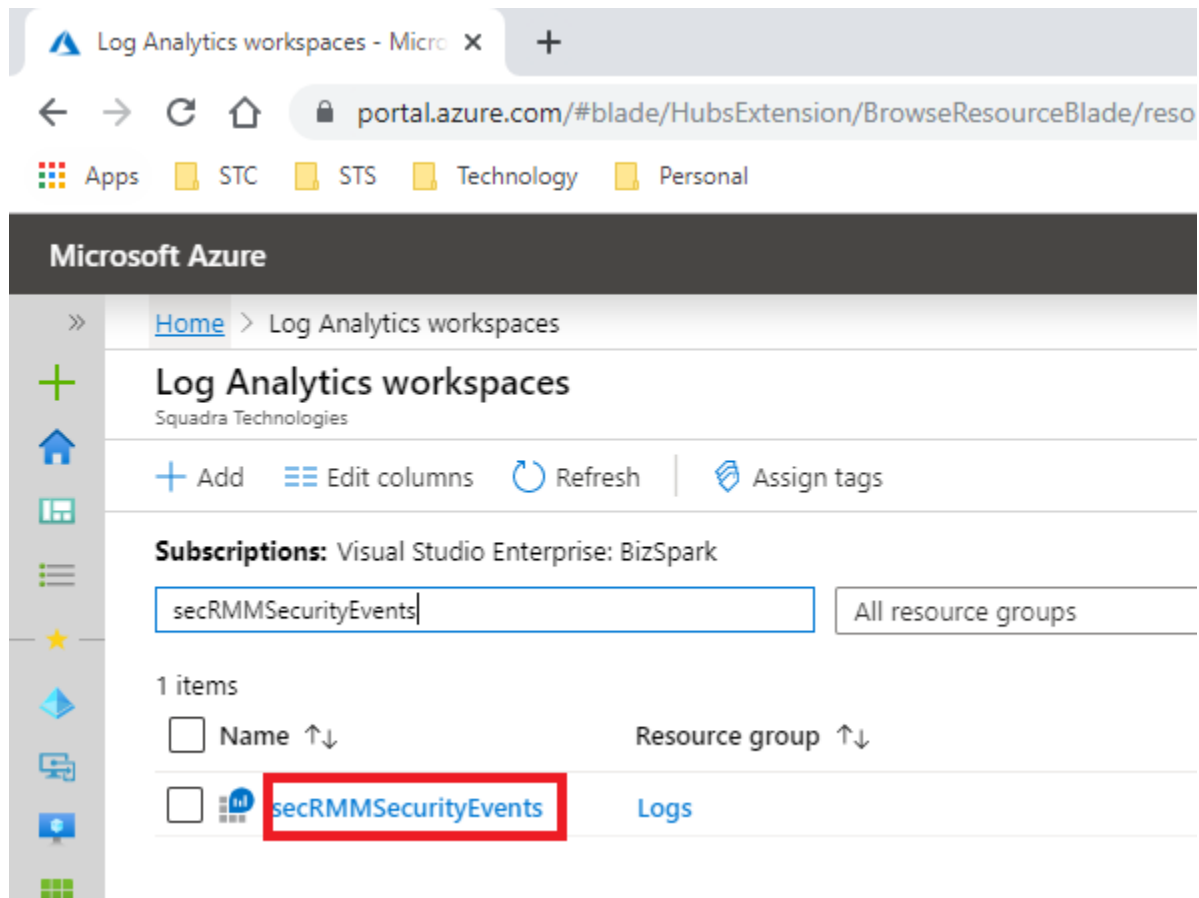
Subscription *
Visual Studio Enterprise: BizSpark ▼

Resource group *
Logs ▼
[Create new](#)

Location *
West US ▼

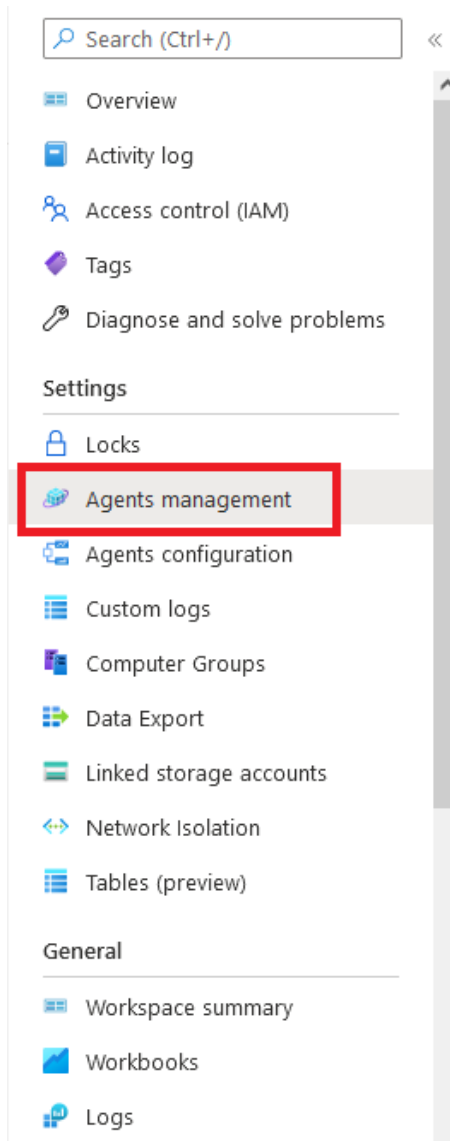
Once the “Log Analytics workspace” is created, click the name (as shown in the screenshot below).

secRMM Defender for Cloud Administrator Guide



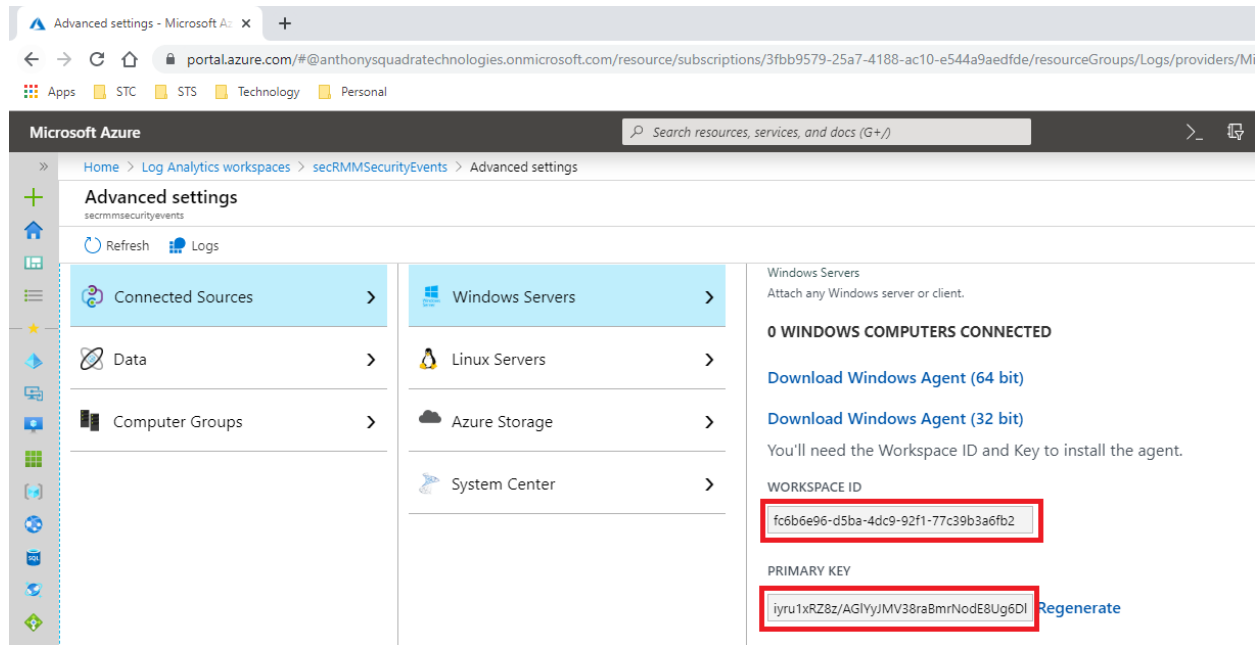
Click the “Agents management” link (as shown in the screenshot below).

secRMM Defender for Cloud Administrator Guide



You will need two values on the Azure web page: **WORKSPACE ID** and **PRIMARY KEY** (as shown in the screenshot below). You will specify these 2 values in the secRMM setup below. These values will tell secRMM where to send the secRMM security events to (see the subsection titled *Configure secRMM to send events to “Azure Log Workspace for secRMM”* below). Use Notepad to copy and paste them to save them for later use.

secRMM Defender for Cloud Administrator Guide



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.

secRMM Defender for Cloud Administrator Guide

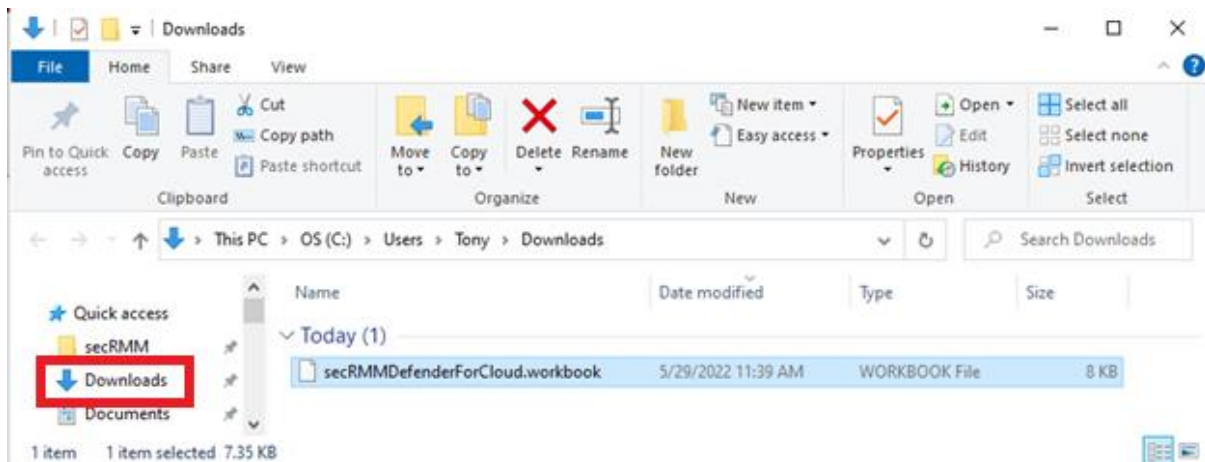
Home >> secRMM >> Downloads >> System Center/Azure >> Azure Defender for Cloud

secRMM Connector to Microsoft Azure Defender for Cloud

Microsoft Azure Defender for Cloud allows you to incorporate removable media security (via secRMM) into your overall security strategy. This web page is what you need to connect the "secRMM security events for removable storage" to **Microsoft Azure Defender for Cloud**. Please follow the setup instructions in the "Defender for Cloud Admin Guide" below to use the secRMM Connector to Microsoft Azure Defender for Cloud.

| Item | Download link |
|------------------------------------|--|
| Defender for Cloud Admin Guide | Defender for Cloud Admin Guide |
| secRMM Defender for Cloud Workbook | secRMM Defender for Cloud Workbook |

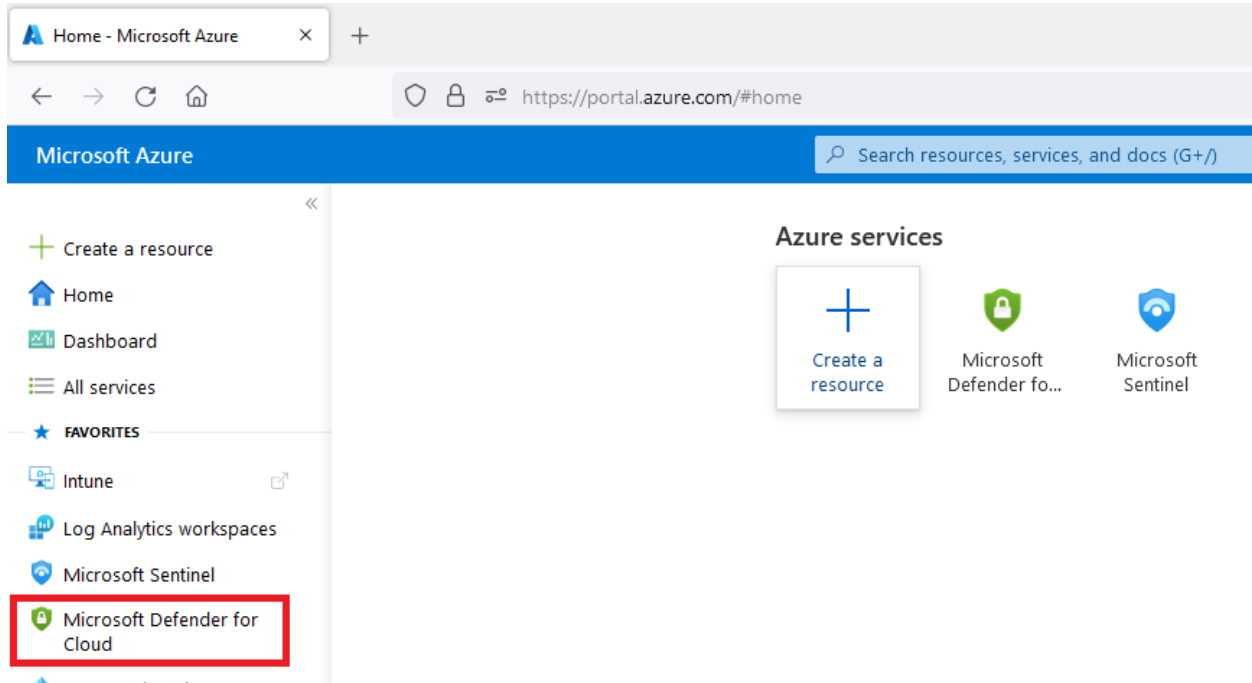
Clicking the 'secRMM Defender for Cloud Workbook' link will download the workbook to your downloads folder as shown in the screenshot below.



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.

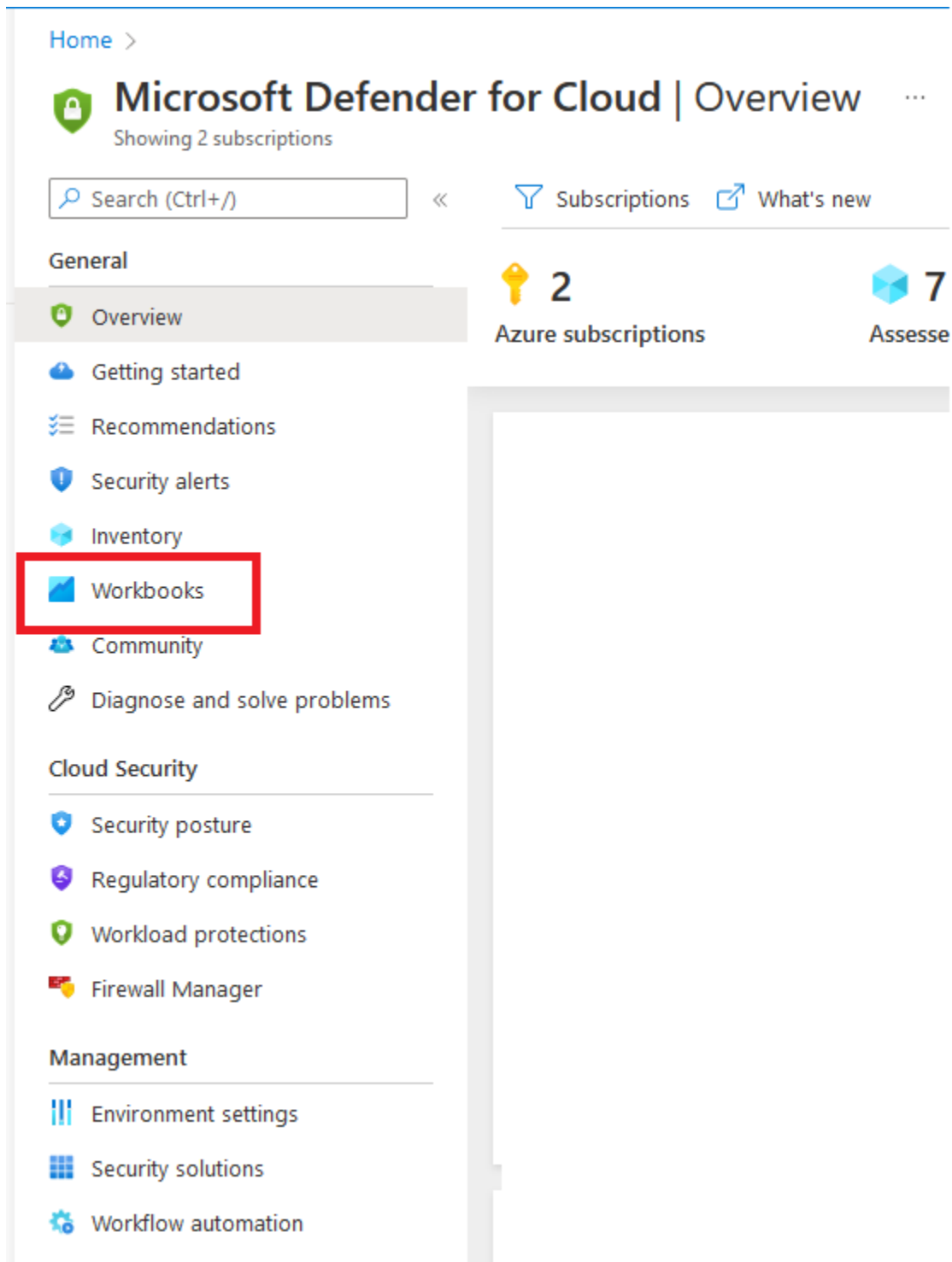
secRMM Defender for Cloud Administrator Guide

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.



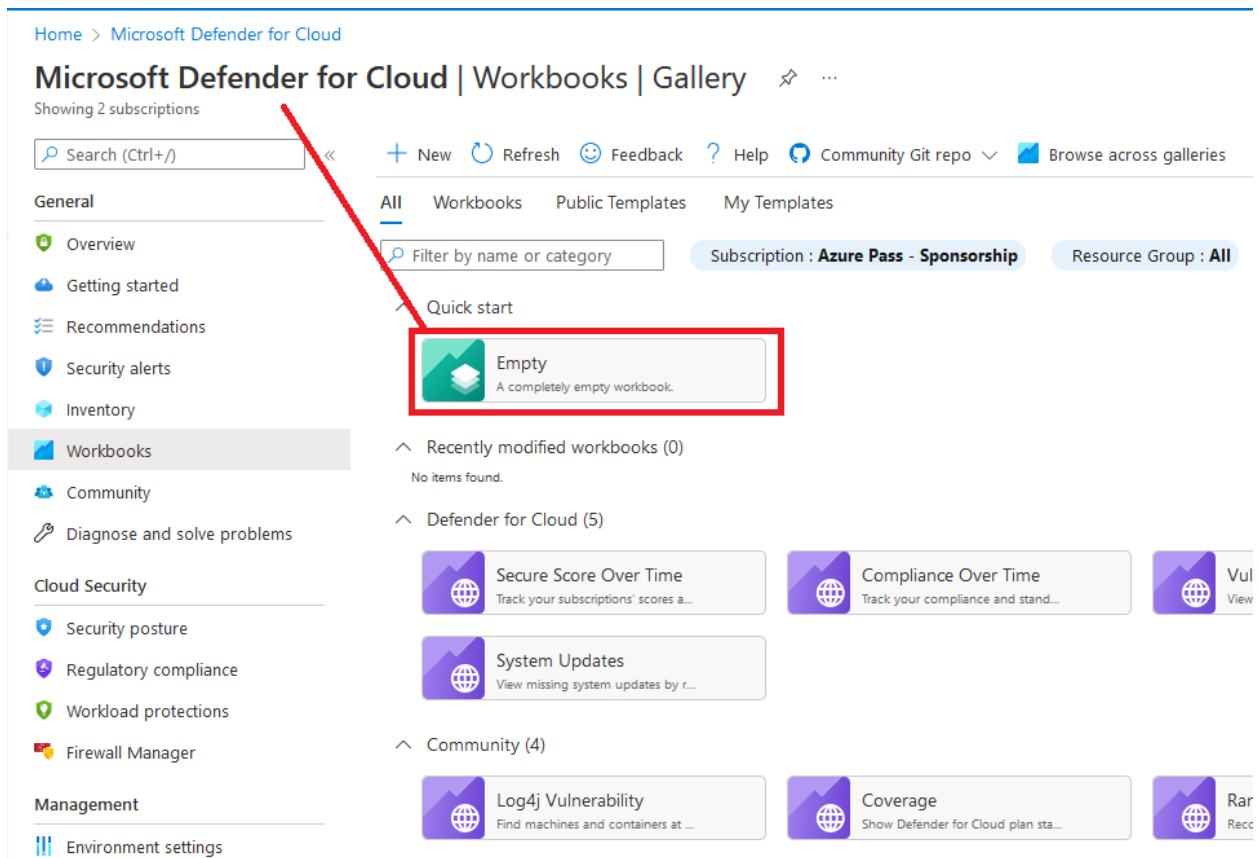
On the 'Microsoft Defender for Cloud' page, click 'Workbooks' as shown in the screenshot below.

secRMM Defender for Cloud Administrator Guide

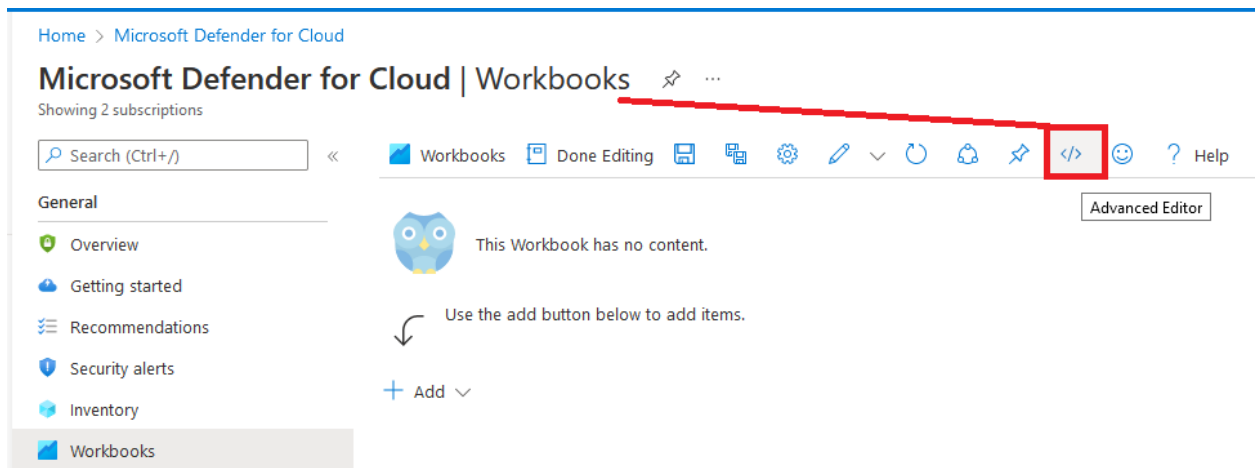


On the 'Microsoft Defender for Cloud Workbooks' page, click the 'Empty' workbook as shown in the screenshot below.

secRMM Defender for Cloud Administrator Guide

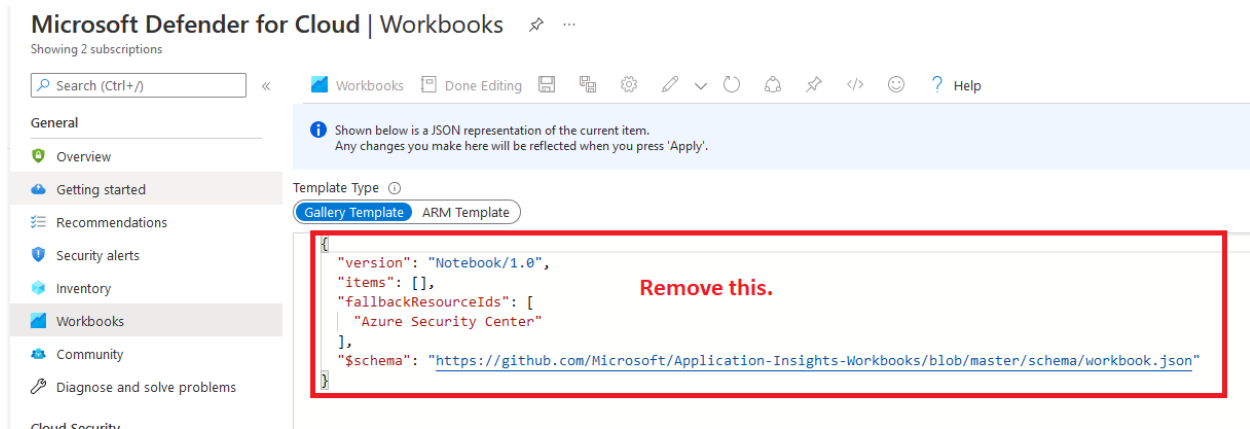


On the page, click the 'Advanced Editor' link as shown in the screenshot below.

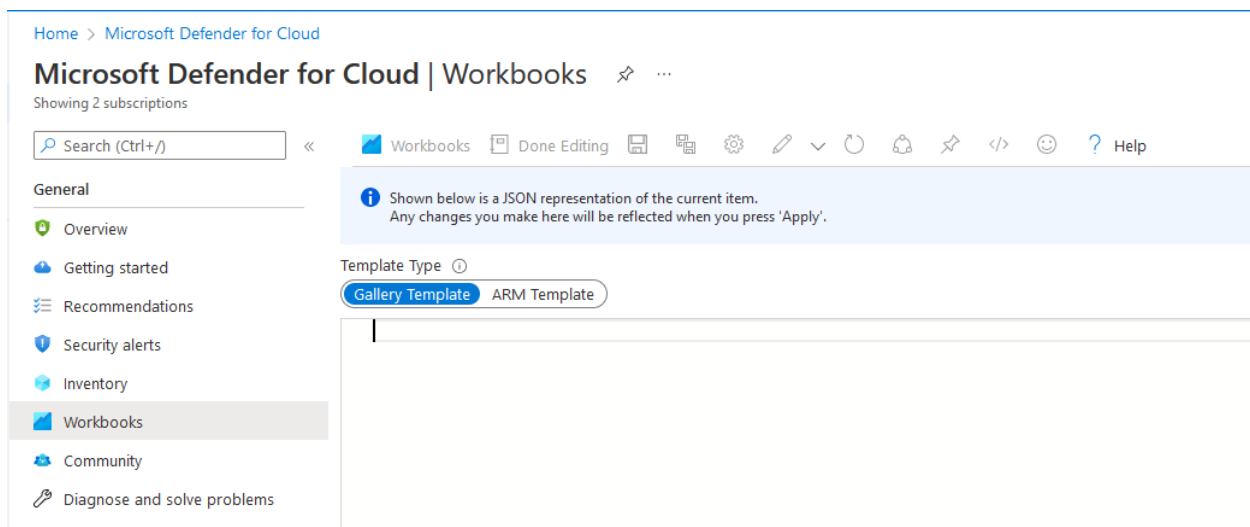


On the page, remove the existing json from the editor as shown in the screenshot below.

secRMM Defender for Cloud Administrator Guide



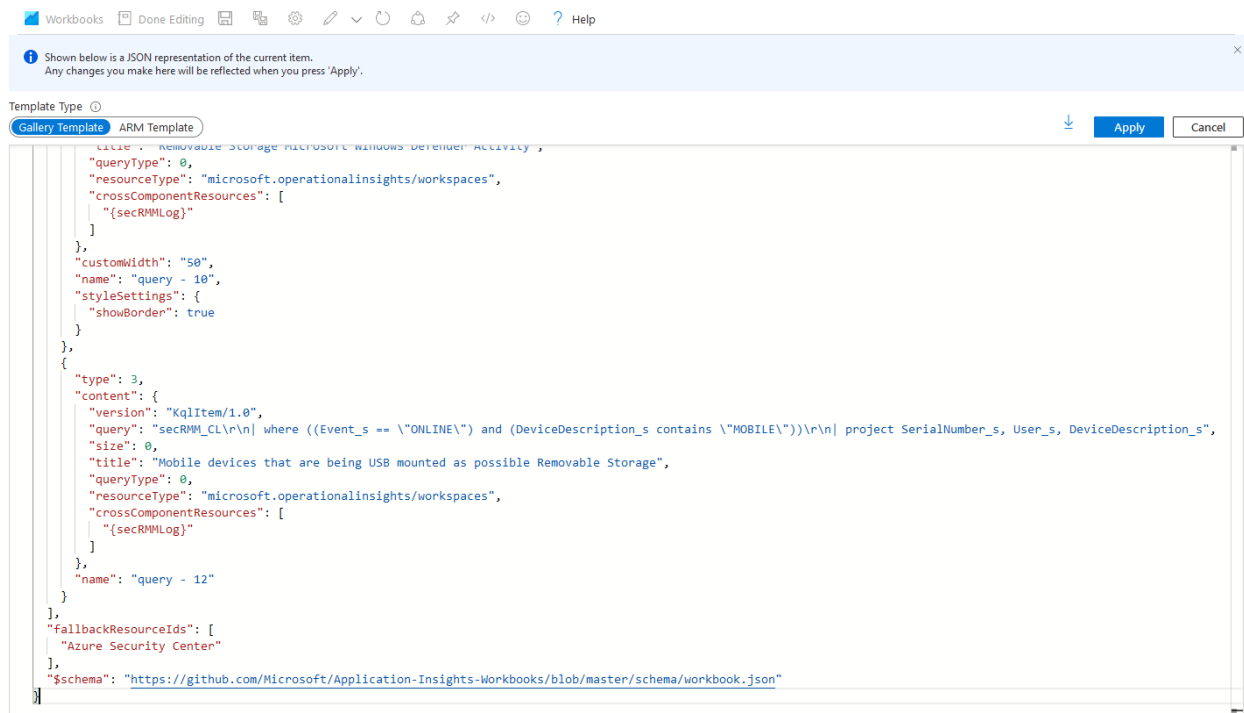
The page will now look like the screenshot below.



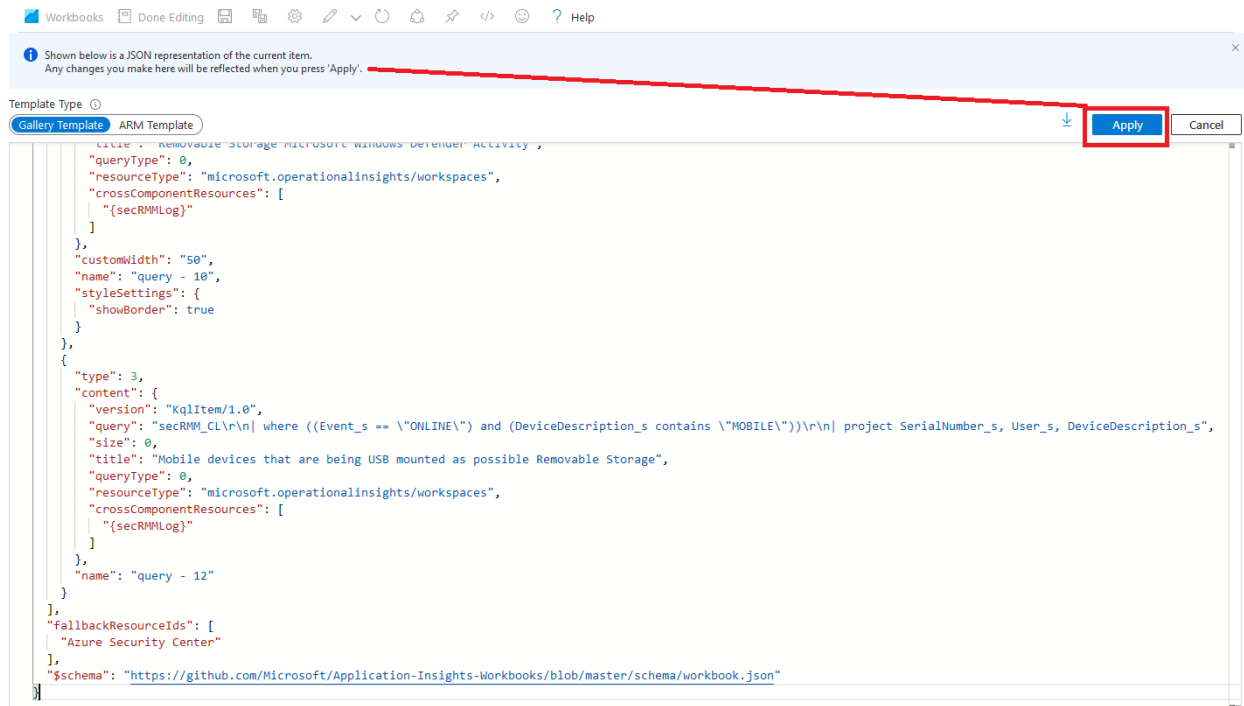
Now, copy (you can just use notepad to open and copy the lines) all the lines in the file named secRMMDefenderForCloud.workbook (which is in your downloads folder from above) and paste all the lines into the page (where you just cleared out all the json).

The page will now look like the screenshot below.

secRMM Defender for Cloud Administrator Guide

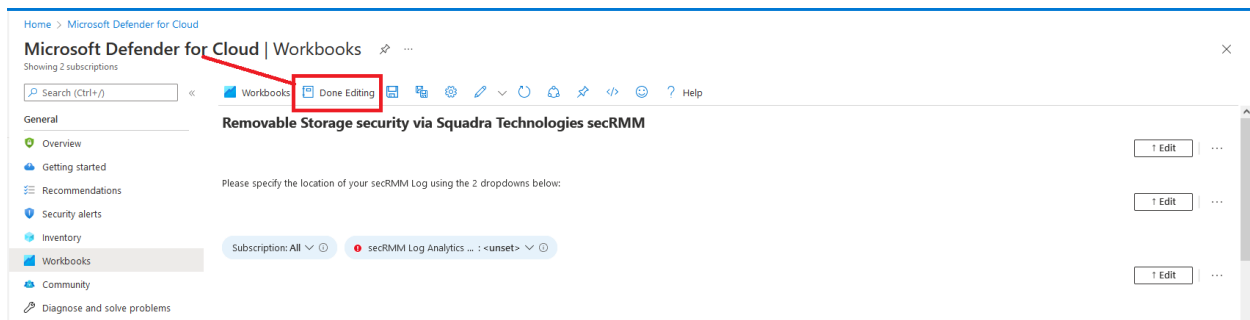


Click the 'Apply' button as shown in the screenshot below.

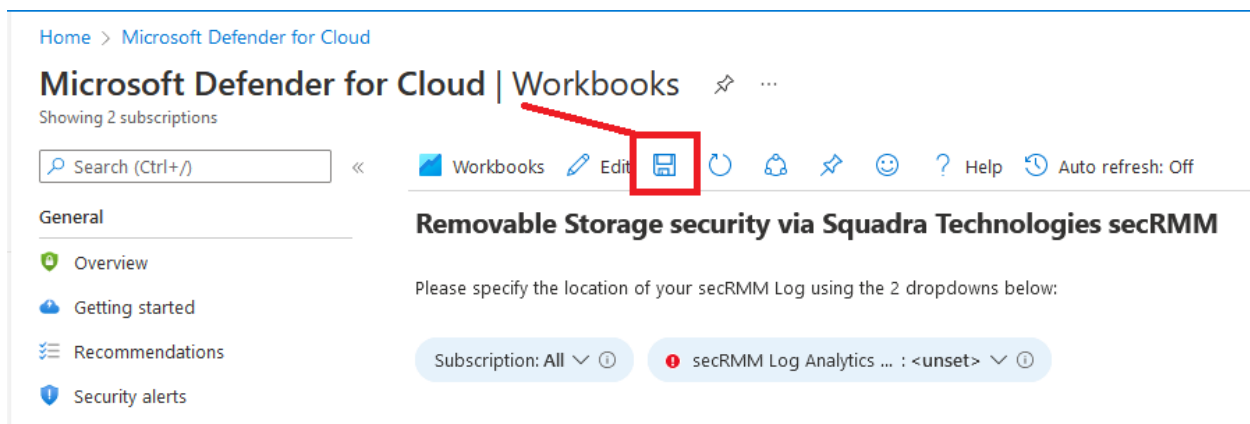


Now click the 'Done Editing' button as shown in the screenshot below.

secRMM Defender for Cloud Administrator Guide



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

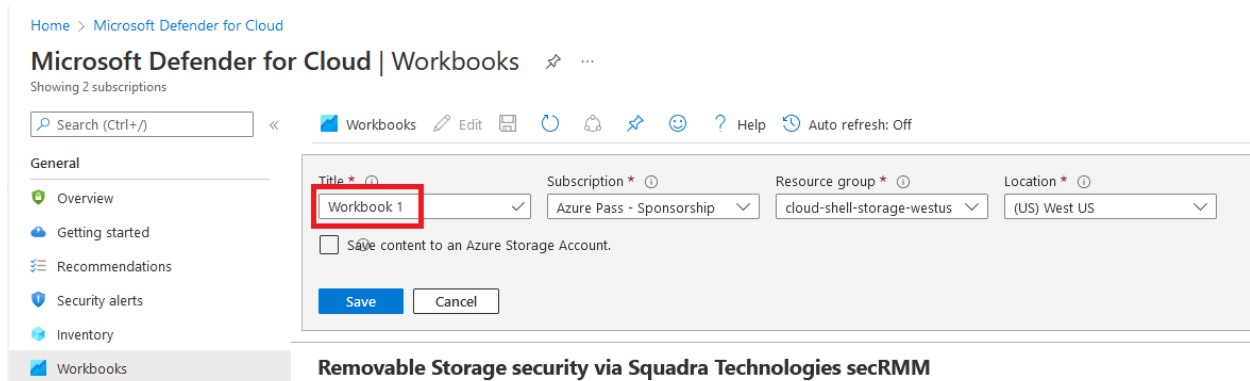


You can name the workbook anything you like.

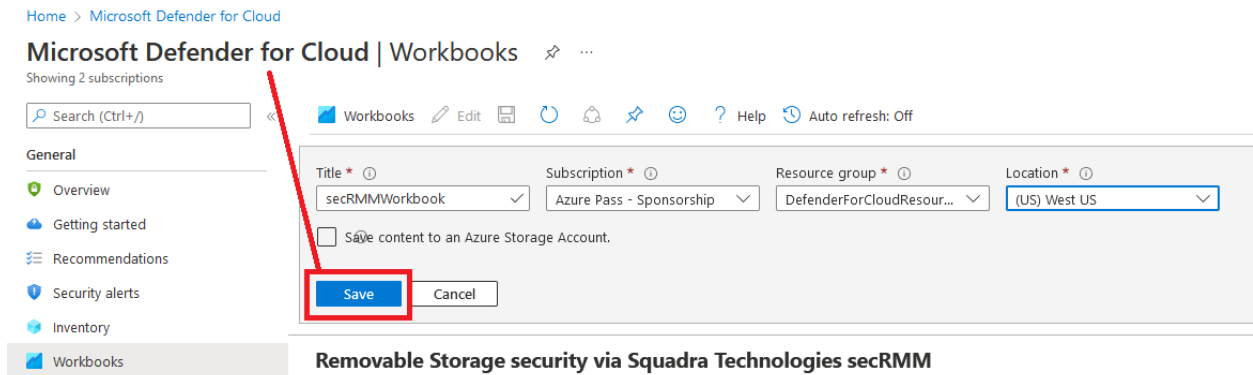
We suggest naming the secRMMWorkbook.

You can also modify the Subscription and/or Resource group and/or Location values to match your Azure tenant.

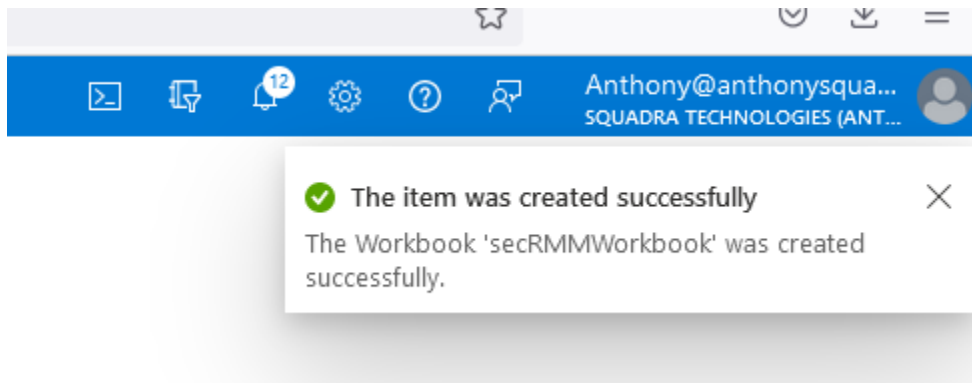
Then, click the 'Save' button as shown in the second screenshot below.



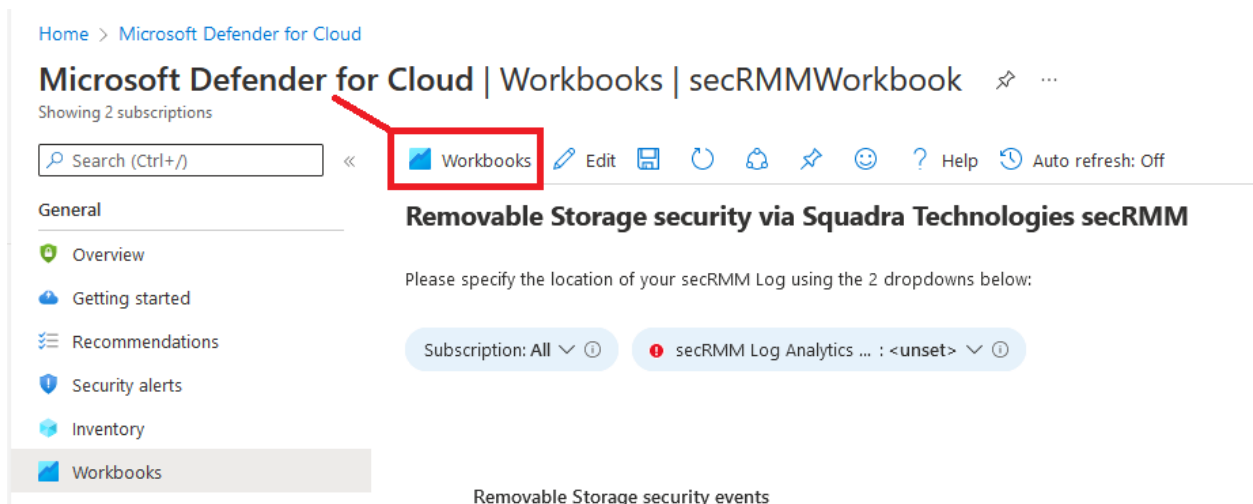
secRMM Defender for Cloud Administrator Guide



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

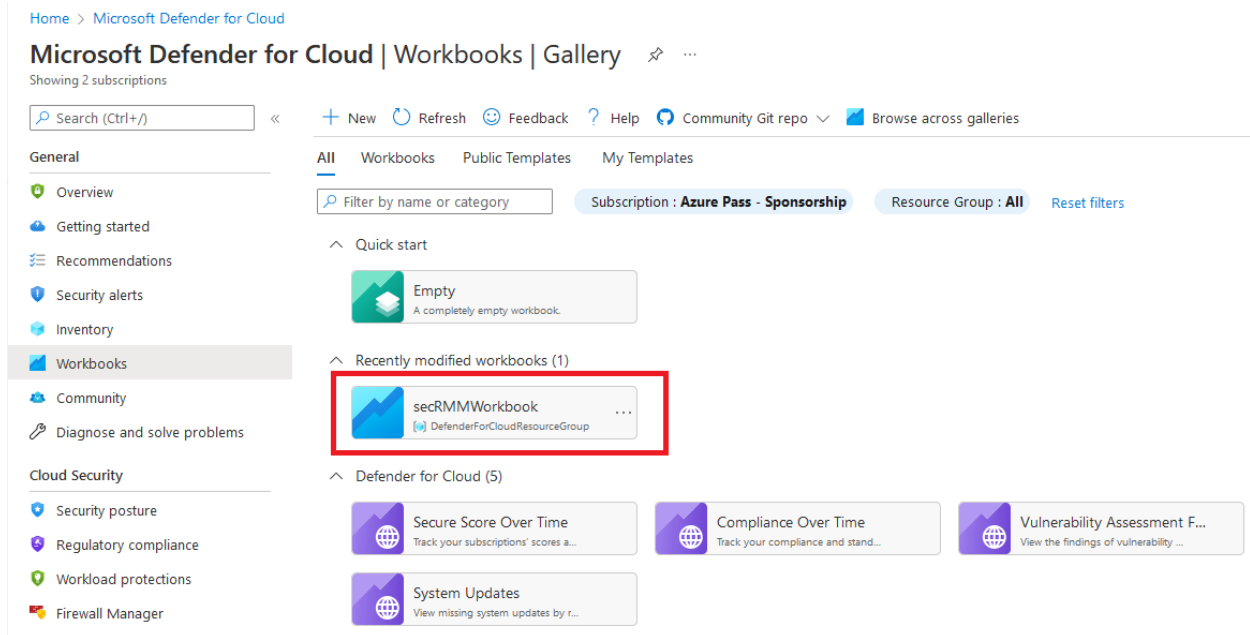


Now, if you click the workbooks button as shown in the screenshot below.



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

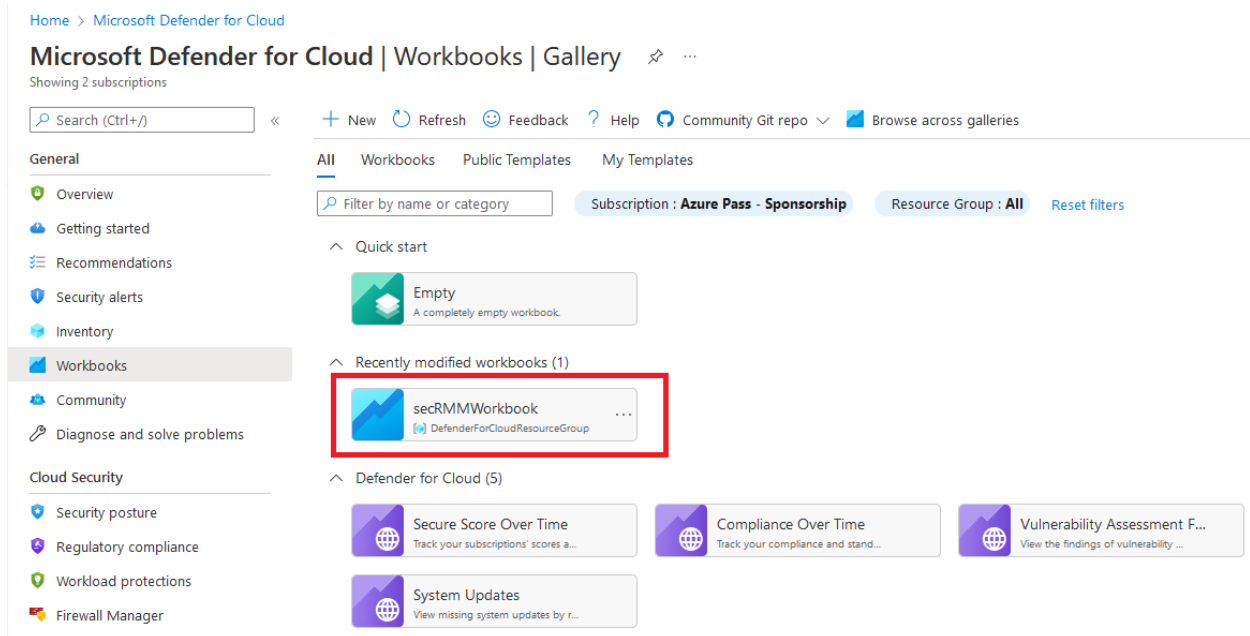
secRMM Defender for Cloud Administrator Guide



Connect “Azure Log Workspace for secRMM” to Microsoft Defender for Cloud

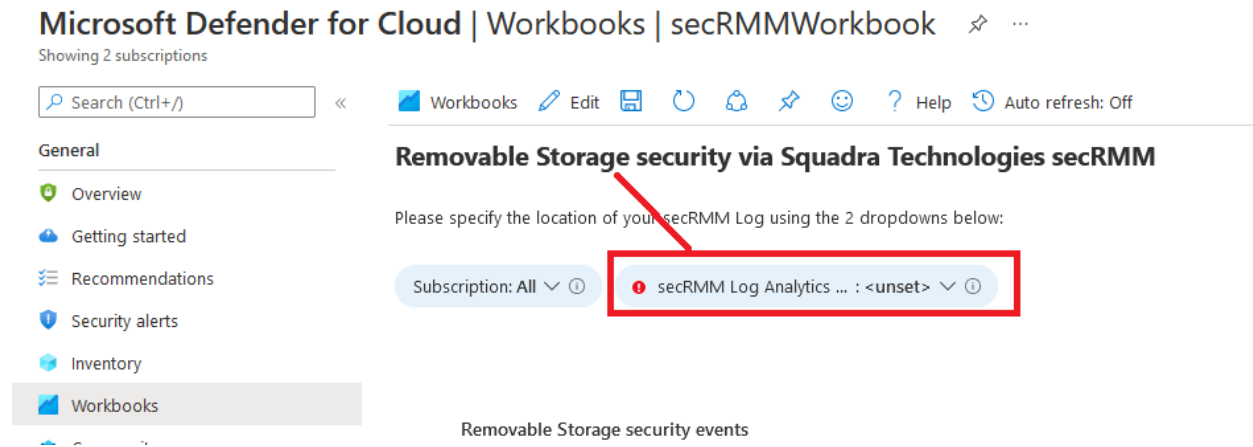
Now that you have created an “Azure Log Workspace for secRMM” (from the subsection above) and you have downloaded and imported the “secRMM Defender for Cloud workbook”, you can connect the “Azure Log Workspace for secRMM” to your “Defender for Cloud workbook for secRMM”.

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

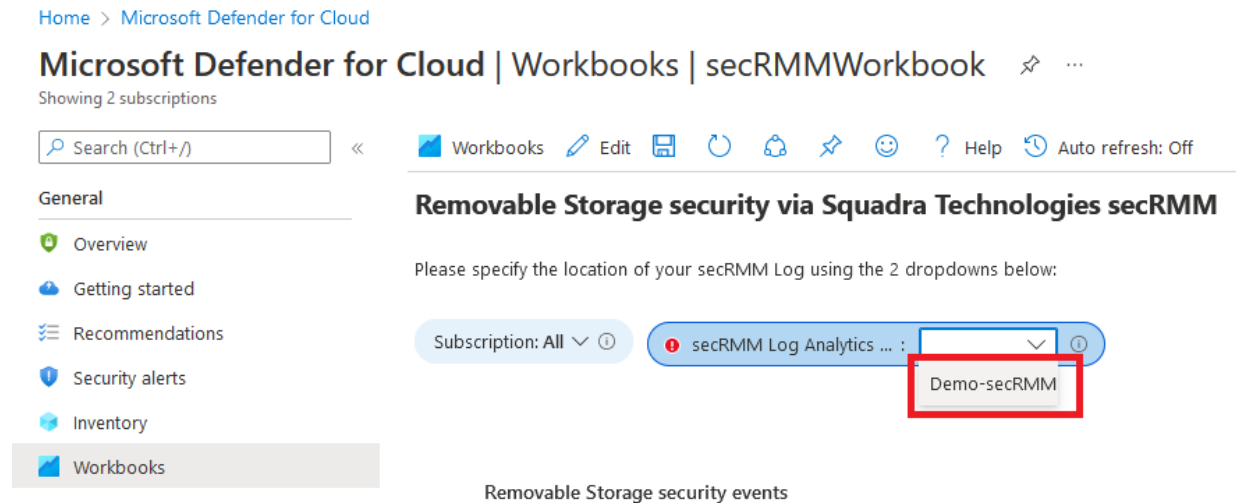


secRMM Defender for Cloud Administrator Guide

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).



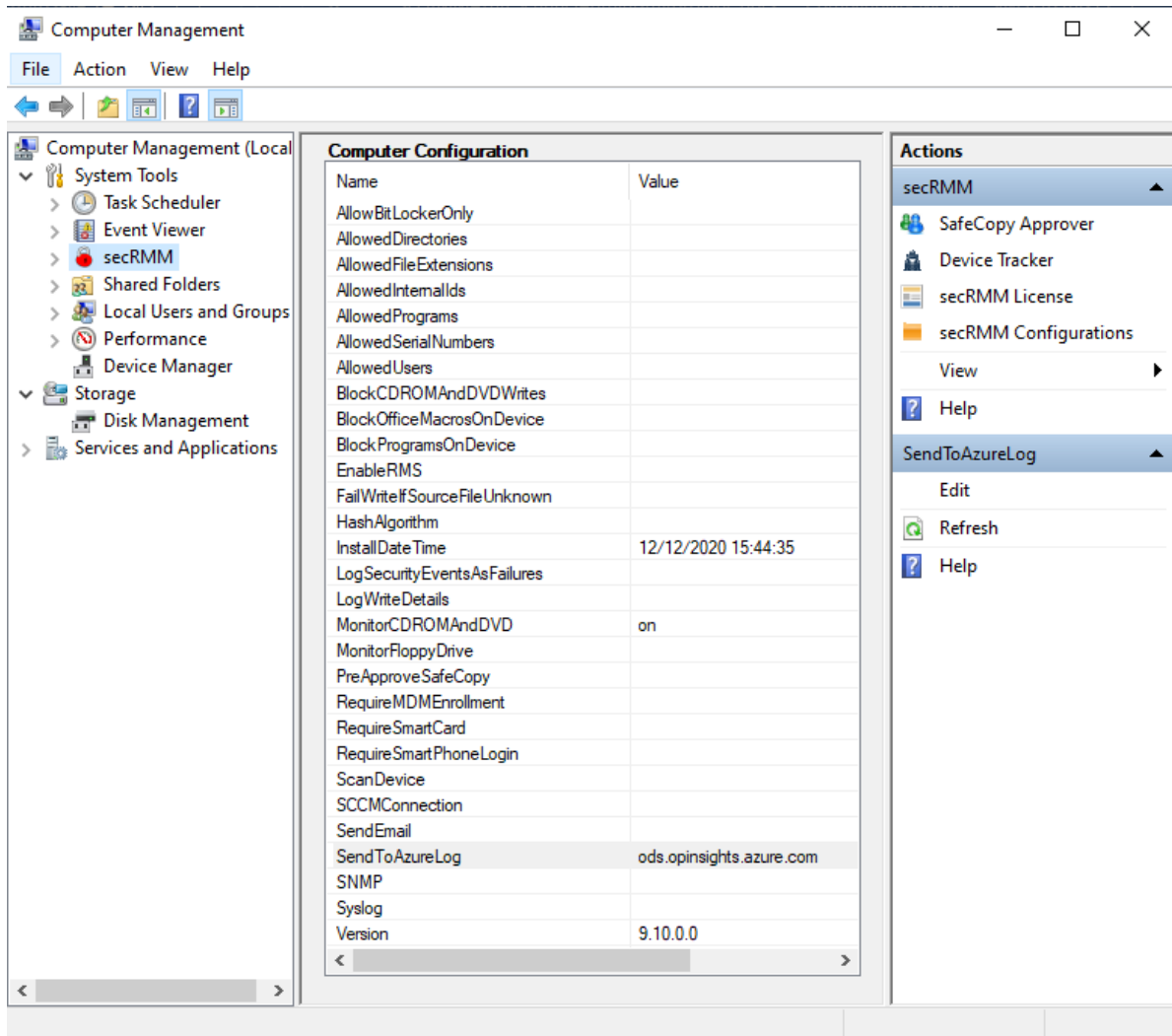
Once you select the workspace, the workbook will be ready to render the security events generated by secRMM. The next section shows how to tell secRMM to send the security events to the 'Azure Log Workspace'.

Configure secRMM to send events to "Azure Log Workspace for secRMM"

The last setup step is to tell secRMM to send its security events to the "Azure Log Workspace". Where you specify this step (i.e. in SCCM, Intune, AD GPO or locally in "Computer Management" console) will depend on how you are managing secRMM in your environment. If you are unsure, please just contact Squadra Technologies support (support@squadratechnologies.com) and we will help you with the setup.

secRMM Defender for Cloud Administrator Guide

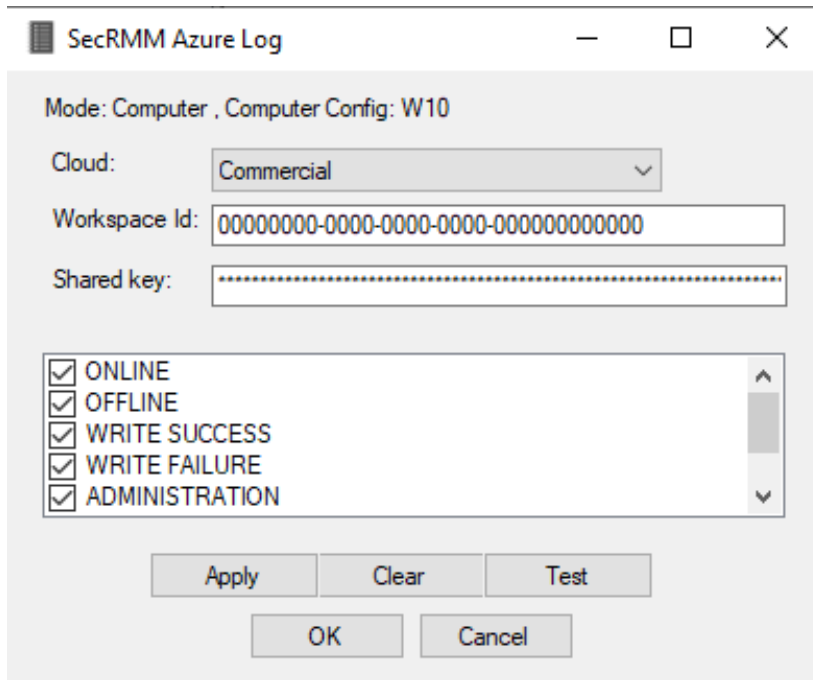
Go into the secRMM interface (i.e. SCCM, Intune, AD GPO or “Computer Management”) and double click the row labeled “SendToAzureLog” (as shown in the screenshot below).



Specify the **WORKSPACE ID** and **PRIMARY KEY** that you copied when you created the “Log Analytics Workspace” in the subsection above titled *Create “Azure Log Workspace for secRMM”* into the secRMM dialog (as shown in the screenshot below). Note that the **PRIMARY KEY** is called “Shared key” in secRMM. Also note that this value is treated like a password and so you will only see asterisks when you paste it into the text field.

Next, in the list of events, select which secRMM security events you want to send to the Azure Log.

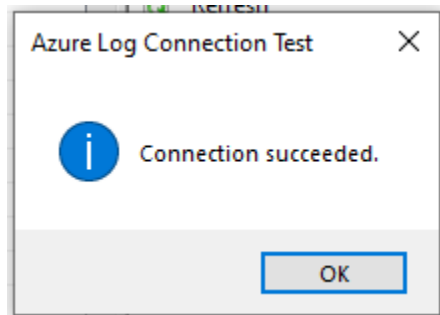
secRMM Defender for Cloud Administrator Guide



The screenshot shows a window titled "SecRMM Azure Log". It contains the following fields and controls:

- Mode: Computer , Computer Config: W10
- Cloud: A dropdown menu with "Commercial" selected.
- Workspace Id: A text box containing "00000000-0000-0000-0000-000000000000".
- Shared key: A text box with a masked key (dots).
- A list of checkboxes with the following labels: ONLINE, OFFLINE, WRITE SUCCESS, WRITE FAILURE, and ADMINISTRATION. All checkboxes are checked.
- Buttons at the bottom: Apply, Clear, Test, OK, and Cancel.

Click the **Apply** button and then the **Test** button. If the test succeeds, you will see the Message box as shown below.



You can now use Azure Defender for Cloud to integrate your USB security into your overall security strategy!

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).

secRMM Defender for Cloud Administrator Guide

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"
```

The screenshot shows the Azure Sentinel Logs interface. The query editor displays the KQL query: `secRMM_CL | where Event_s == "ONLINE"`. The results table shows one event:

| TimeGenerated [UTC] | Computer | RawData | Event_s | Time_s | User_s |
|----------------------------|----------|---------|---------|-----------------------|----------|
| 11/13/2019, 8:01:01.910 PM | W10 | | ONLINE | 11/13/2019 8:00:59 PM | W10\Tony |

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)
```

secRMM Defender for Cloud Administrator Guide

The screenshot shows the Azure Sentinel Logs interface. The left sidebar contains navigation options: Home, Overview, Logs, News & guides, Threat management, Incidents, Workbooks, Hunting, and Notebooks. The main pane displays a KQL query in the 'Schema' tab:

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

The query is highlighted with a red box. Below the query, the results are shown in a table with one row: ERRORS, 1. The time range is set to 'Last 24 hours'.

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
```

The screenshot shows the Azure Sentinel Logs interface. The left sidebar contains navigation options: Home, Overview, Logs, News & guides, Threat management, Incidents, Workbooks, Hunting, and Notebooks. The main pane displays a KQL query in the 'Schema' tab:

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

The query is highlighted with a red box. Below the query, the results are shown in a table with two columns: User_s and count_. The results are: W10/Tony, 4. The time range is set to 'Last hour'.

secRMM Defender for Cloud Administrator Guide

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 Defender for Cloud Administrator Guide

secRMM Event Viewer: localhost, event log secRMM

Row:

| | 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"))
```

secRMM Defender for Cloud Administrator Guide

| | | | | | |
|--|----------|--|---|---|---|
| secRMM Event Viewer: localhost, event log secRMM | | | — | □ | × |
| Row: 38 Previous Next | | | | | |
| | 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"

| | | | | | |
|--|------------------------|--|---|---|---|
| secRMM Event Viewer: localhost, event log secRMM | | | — | □ | × |
| Row: 25 Previous Next | | | | | |
| | 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\Harddisk Volume 11 | | | |
| | 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\070007089784F7226654&0 | | | |
| | 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 Defender for Cloud Administrator Guide

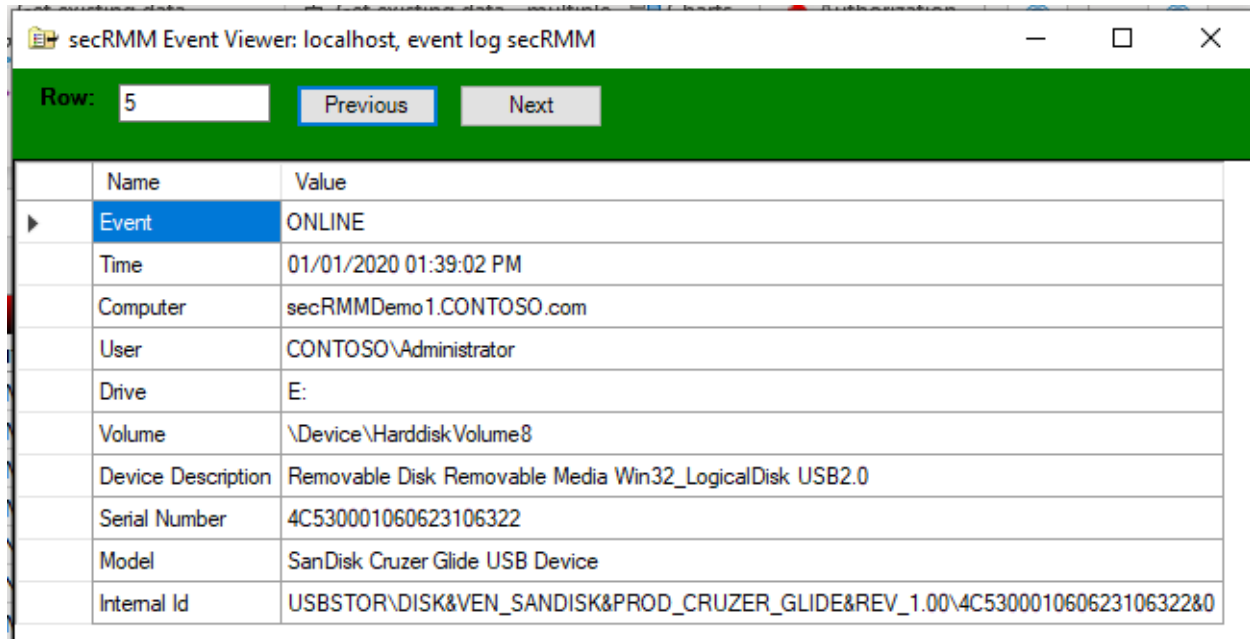
```
secRMM_CL | where ((Event_s == "BLOCK MACROS ON DEVICE ACTIVE") or (Event_s ==  
"BLOCK PROGRAMS ON DEVICE ACTIVE")) | summarize count() by User_s
```

| secRMM Event Viewer: localhost, event log secRMM | | |
|--|--------------------|--|
| Row: | 11 | Previous Next |
| | 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"))
```

secRMM Defender for Cloud Administrator Guide



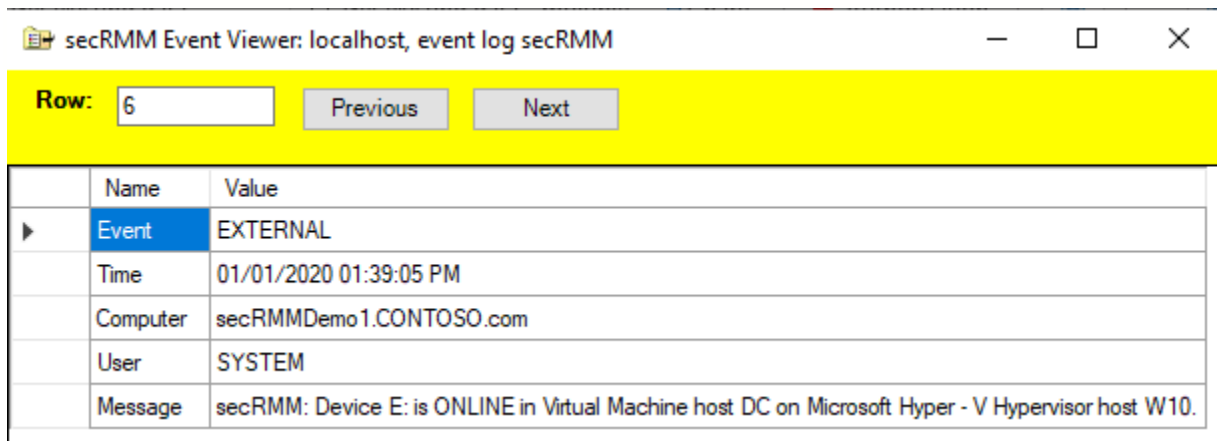
The screenshot shows the 'secRMM Event Viewer' window for 'localhost, event log secRMM'. The 'Row' is set to 5. The event details are as follows:

| Name | Value |
|--------------------|--|
| Event | ONLINE |
| Time | 01/01/2020 01:39:02 PM |
| Computer | secRMMDemo1.CONTOSO.com |
| User | CONTOSO\Administrator |
| Drive | E: |
| Volume | \Device\Harddisk Volume8 |
| 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"))
```



The screenshot shows the 'secRMM Event Viewer' window for 'localhost, event log secRMM'. The 'Row' is set to 6. The event details are as follows:

| Name | Value |
|----------|--|
| Event | EXTERNAL |
| Time | 01/01/2020 01:39:05 PM |
| Computer | secRMMDemo1.CONTOSO.com |
| User | SYSTEM |
| Message | secRMM: Device E: is ONLINE in Virtual Machine host DC on Microsoft Hyper - V Hypervisor host W10. |

Event on the virtual machine

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

secRMM Defender for Cloud Administrator Guide

| | | |
|--|--------------------|---|
| secRMM Event Viewer: localhost, event log secRMM | | |
| Row: 7 Previous Next | | |
| | Name | Value |
| ▶ | Event | ONLINE |
| | Time | 01/01/2020 01:39:06 PM |
| | Computer | DC.CONTOSO.com |
| | User | CONTOSO\Administrator |
| | Drive | SECRMMDEMO1^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 |
| | Additional Info | Hypervisor: Microsoft Hyper - V, Hypervisor host: W10, Device mounted on: SECRMMDEMO1:AF_UNSPEC:0.0.88.17 |

Show mobile devices that are being USB mounted

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

| | | |
|--|--------------------|---|
| secRMM Event Viewer: archive file X:\temp.evtx | | |
| Row: 8 Previous Next | | |
| | 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"))
```

secRMM Defender for Cloud Administrator Guide

| secRMM Event Viewer: archive file X:\temp.evtx | |
|--|--|
| Row: 10 | Previous Next |
| 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. |

Azure Log Analytics secRMM schema

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

| | |
|---------------------------|-----------------------------|
| Custom Logs | |
| secRMM_CL | |
| t AdditionalProgramInfo_s | t PropertyOperationStatus_s |
| t Computer | t PropertyValue_s |
| t ConfigurationTarget_s | t RawData |
| t DeviceDescription_s | t SerialNumber_s |
| t Drive_s | t SourceFileLastWrite_s |
| t Event_s | t SourceFileSize_s |
| t InternalID_s | t SourceFile_s |
| t ManagementGroupName | t SourceSystem |
| t Message | t TargetFile_s |
| t Model_s | ⊙ TimeGenerated |
| t PreviousPropertyValue_s | t Time_s |
| t ProgramName_s | t Type |
| t ProgramPID_s | t UserSID_s |
| t PropertyAction_s | t User_s |
| t PropertyName_s | t Volume_s |

Descriptions

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

secRMM Defender for Cloud Administrator Guide

| | |
|---------------------------|---|
| 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.

secRMM Defender for Cloud Administrator Guide

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 7575 West Washington Ave. Suite 127-252 Las Vegas, NV 89128 USA |
| Web site | http://www.squadratechnologies.com/ |