squadra
technologies

Security Removable Media Manager

connector to

Azure Monitor

Version 9.11.26.0
(January 2024)

Protect your valuable data

Contents

Introduction

Description

Microsoft Azure Monitor is a monitoring solution for collecting, analyzing, and responding to monitoring data from your cloud and on-premises environments.

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 Azure Monitor instance. This allows you to see the security events that secRMM generates within Azure Monitor. 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 Azure Monitor" to refer to this secRMM to Azure Monitor 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 Azure Monitor?

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 Azure Monitor 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 Azure Monitor", 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).
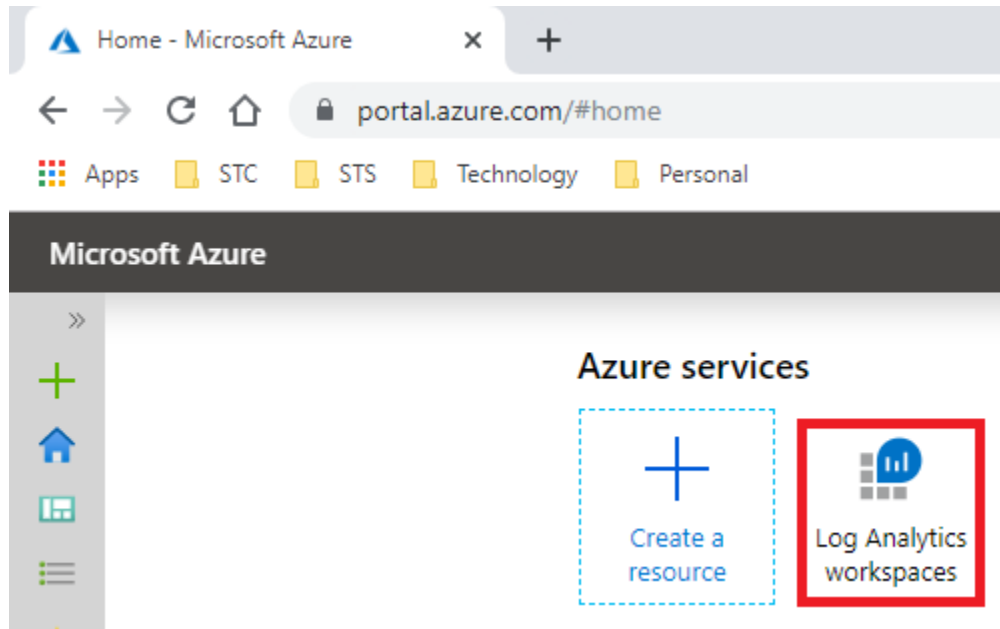
Within your Azure "Log Analytics workspaces", click the Add link (as shown in the screenshot below).
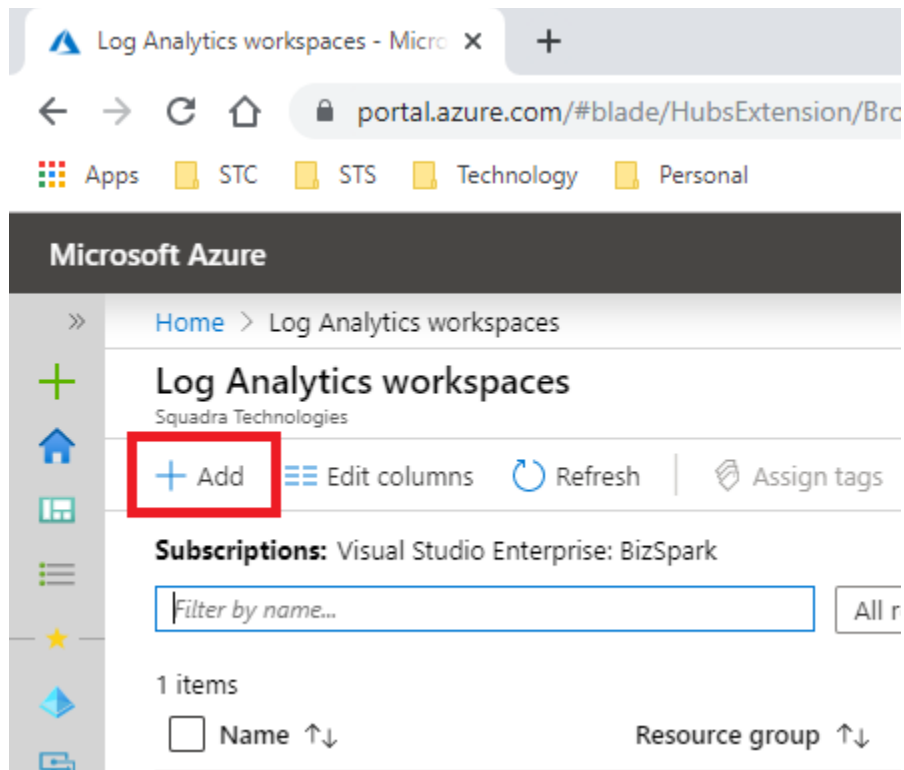
Fill out the form (as shown in the screenshot below).
Note that the values you specify here will be different based on your Azure environment.

Once the "Log Analytics workspace" is created, click the name (as shown in the screenshot below).
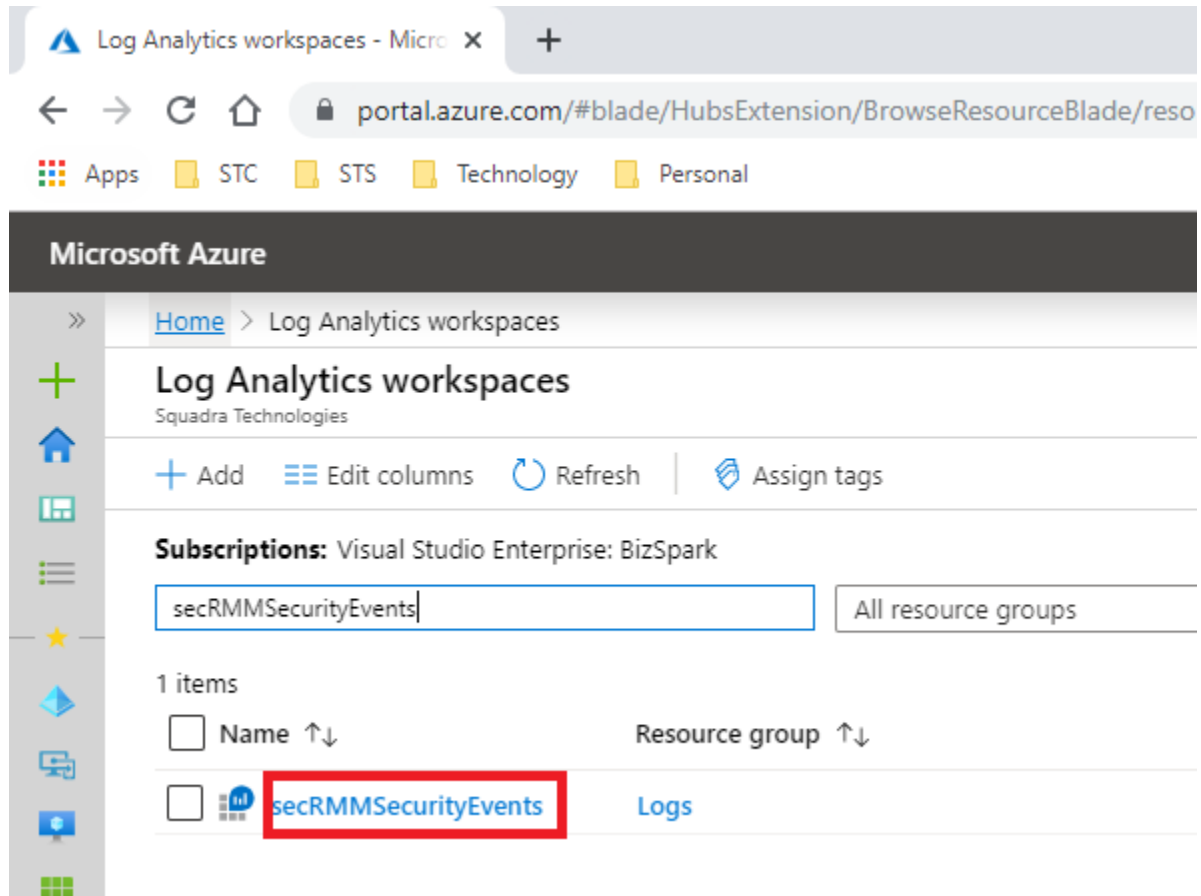
Click the "Agents management" link (as shown in the screenshot below).
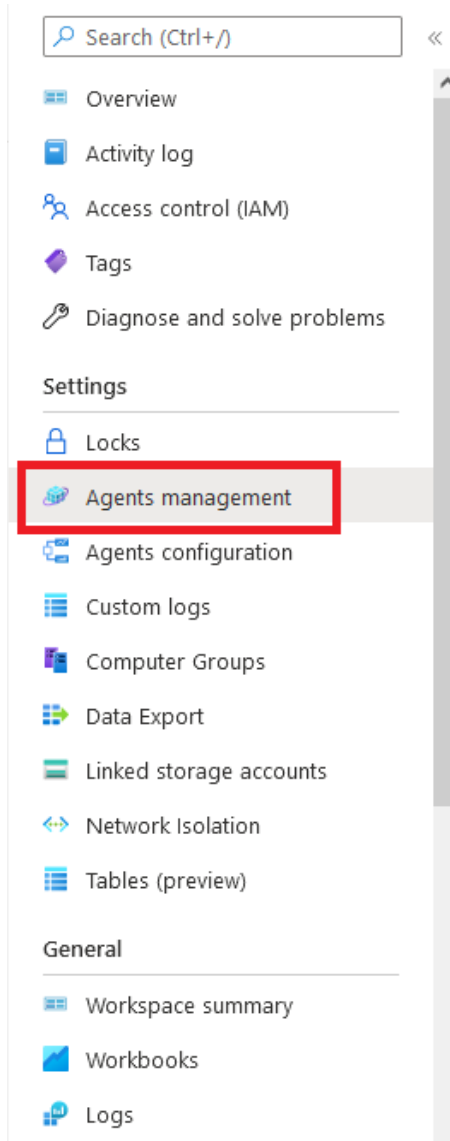
You will need two values on the Azure web page: **WORKSPACE ID** and **PRIMARY KEY** (as shown in the screenshot below). You will specify these 2 values in the secRMM setup below. These values will tell secRMM where to send the secRMM security events to (see the subsection titled *Configure secRMM to send events to "Azure Log Workspace for secRMM"* below). Use Notepad to copy and paste them to save them for later use.
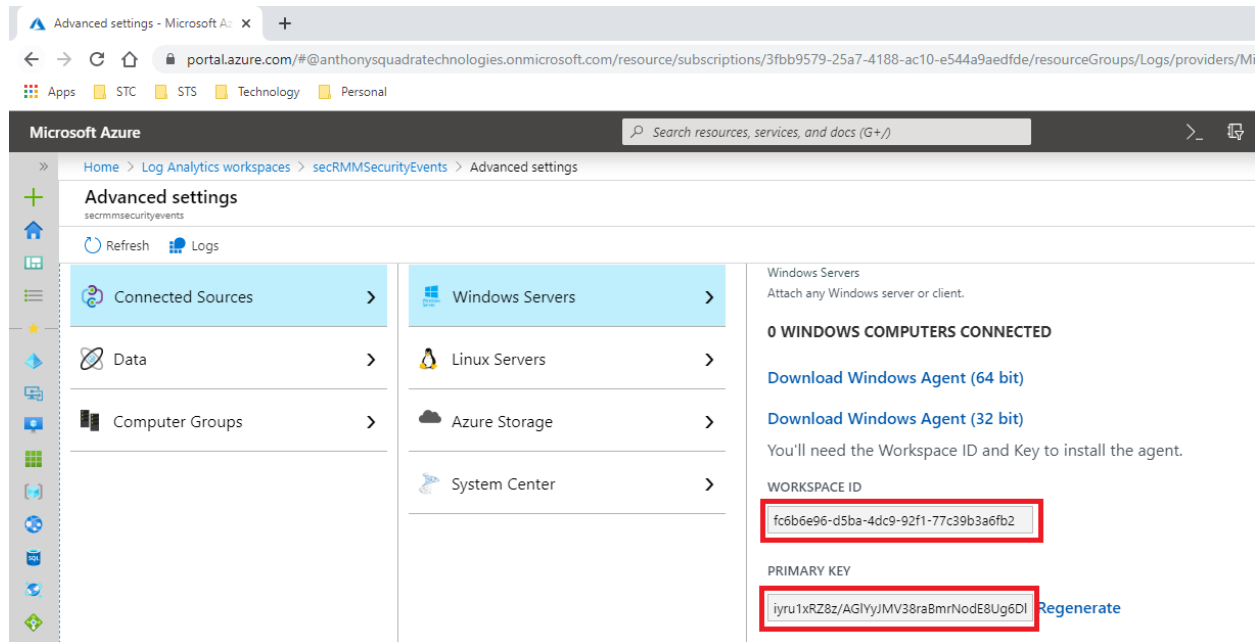
Download and import the 'secRMM Azure Monitor Workbooks'

You download the 'secRMM Azure Monitor Workbooks' from the Squadra technologies web site at: secRMM Azure Monitor Integration by clicking the 'secRMMAzureWorkbooks.zip' link as shown in the screenshot below.

Clicking the 'secRMMAzureWorkbooks.zip' link will download the workbooks to your downloads folder as shown in the screenshot below.
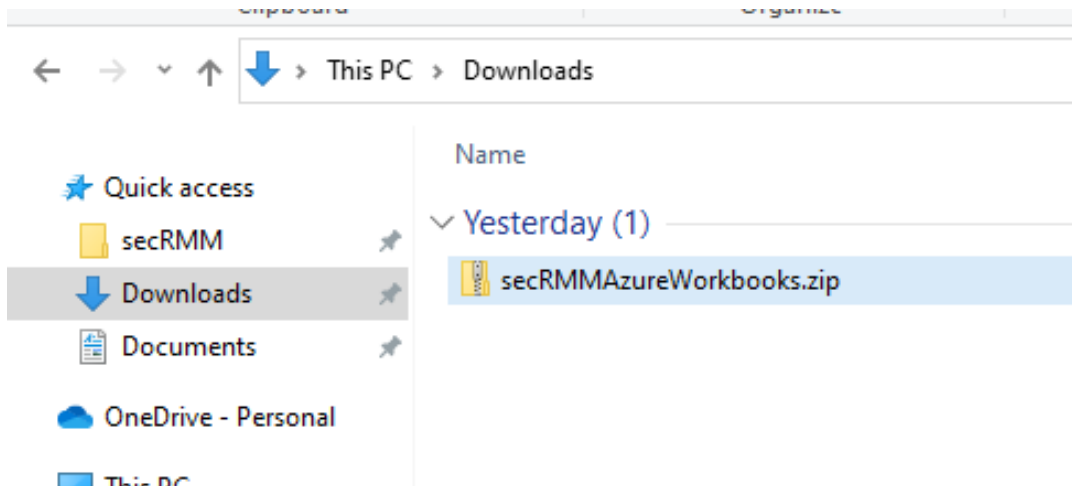
The next few steps will take the 'secRMM Azure Monitor Workbooks' (i.e. the files within the zip file you just downloaded) and import (load) it into your Azure Monitor instance within your Azure tenant. There currently is no nice import function for this but hopefully, eventually, Microsoft will create one.

Go to your Azure portal and select your Monitor instance as shown in the screenshot below. If you do not see 'Monitor' in your Azure portal home page, you can do a search for it using the 'Search resources, services and docs' feature.
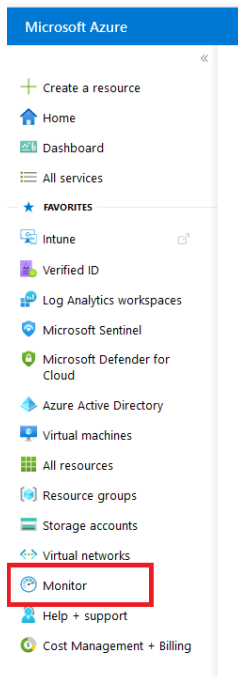
On the 'Monitor' page, click 'Workbooks' as shown in the screenshot below.
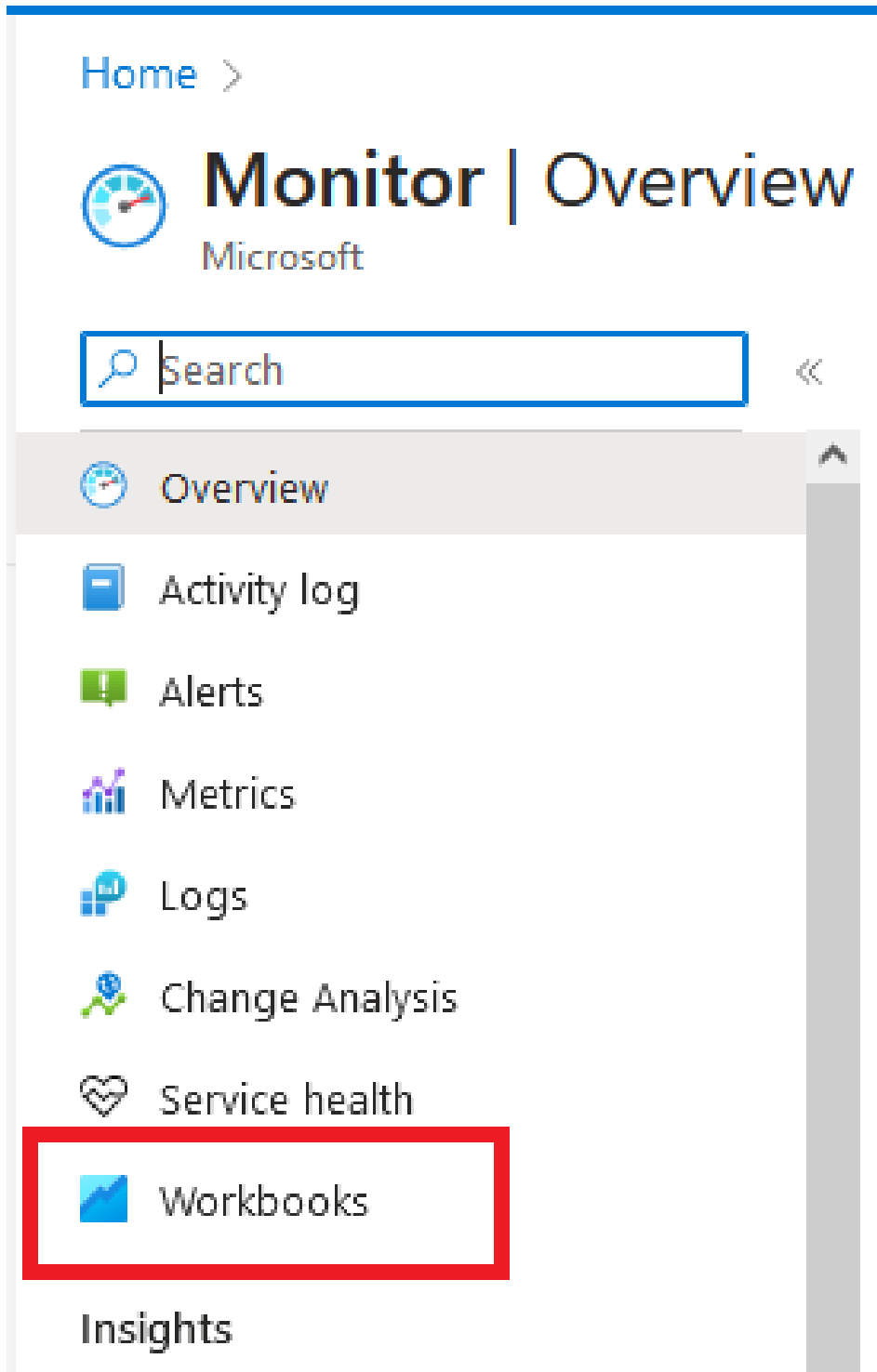
On the 'Monitor | Workbooks | Gallery' page, click the 'Empty' workbook as shown in the screenshot below.
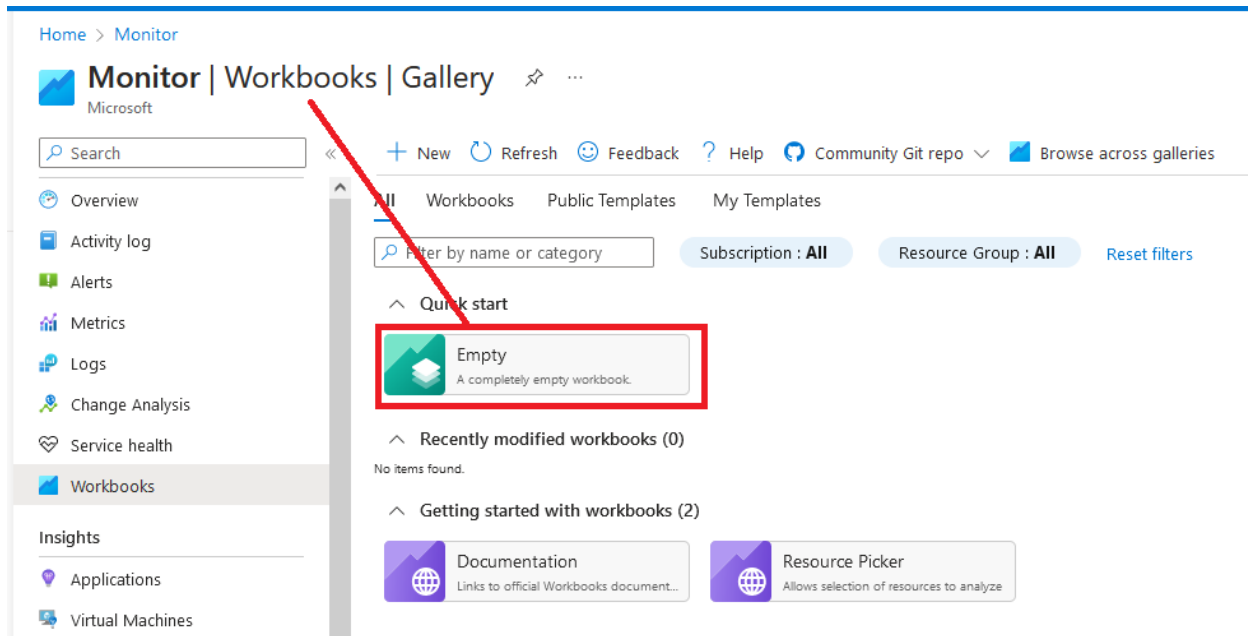
On the page, click the 'Advanced Editor' link as shown in the screenshot below.
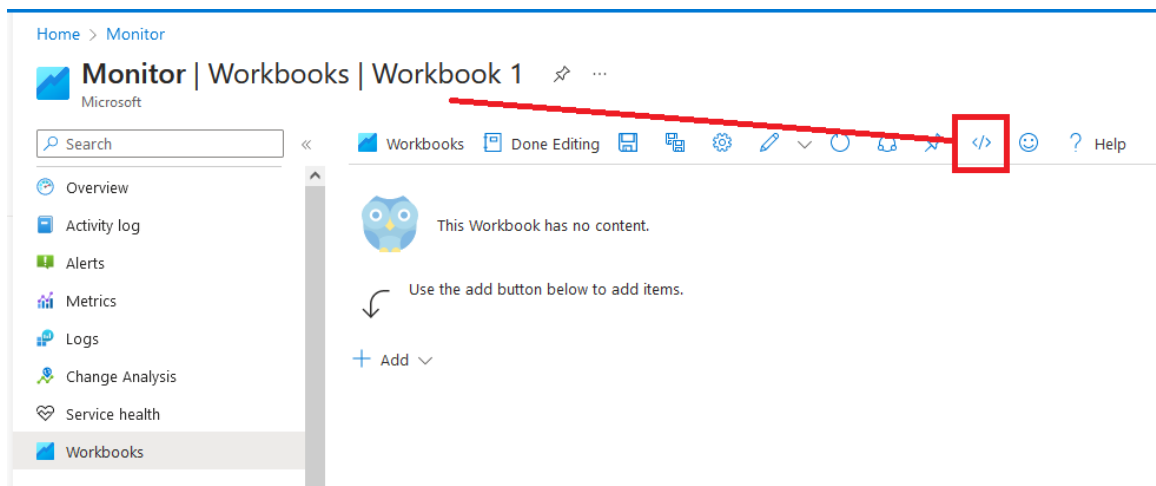
On the page, remove the existing json from the editor as shown in the screenshot below.

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 each file within secRMMAzureWorkbooks.zip and paste all the lines into the page (where you just cleared out all the json.
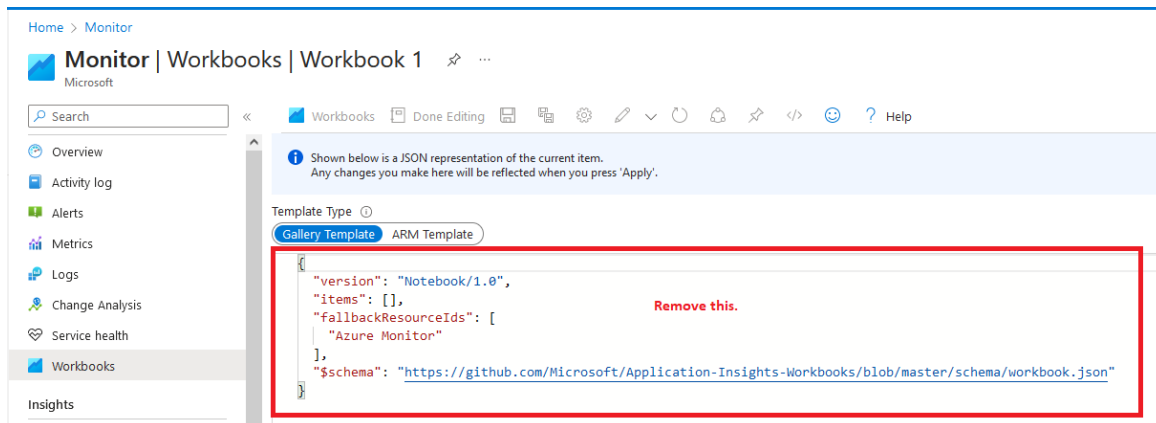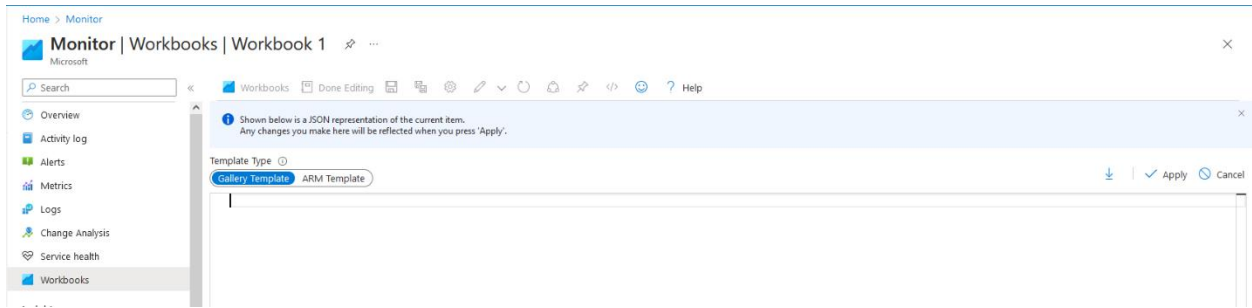
The page will now look like the screenshot below.

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

```
            title : "Removable Storage Microsoft Windows Defender Activity",
            "queryType": 0,
            "resourceType": "microsoft.operationalinsights/workspaces",
            "crossComponentResources": [
              "{secRMMLog}"
            ]
          },
          "customWidth": "50",
          "name": "query - 10",
          "styleSettings": {
            "showBorder": true
          }
        },
        {
          "type": 3,
          "content": {
            "version": "KqlItem/1.0",
            "query": "secRMM_CL\r\n| where ((Event_s == \"ONLINE\") and (DeviceDescription_s contains \"MOBILE\"))\r\n| project SerialNumber_s, User_s, DeviceDescription_s",
            "size": 0,
            "title": "Mobile devices that are being USB mounted as possible Removable Storage",
            "queryType": 0,
            "resourceType": "microsoft.operationalinsights/workspaces",
            "crossComponentResources": [
              "{secRMMLog}"
            ]
          },
          "name": "query - 12"
        }
      ],
      "fallbackResourceIds": [
        "Azure Security Center"
      ],
      "$schema": "https://github.com/Microsoft/Application-Insights-Workbooks/blob/master/schema/workbook.json"
}
```

Now click the 'Done Editing' button as shown in the screenshot below.
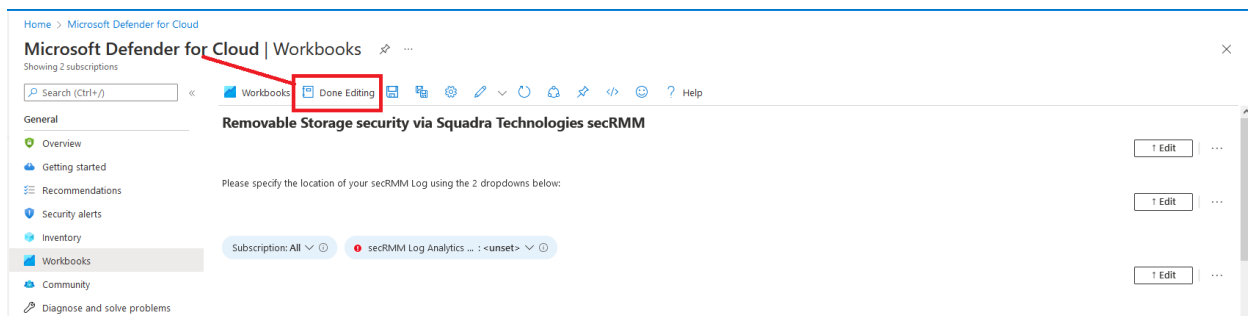
Now click the 'Save' button as shown in the screenshot below.
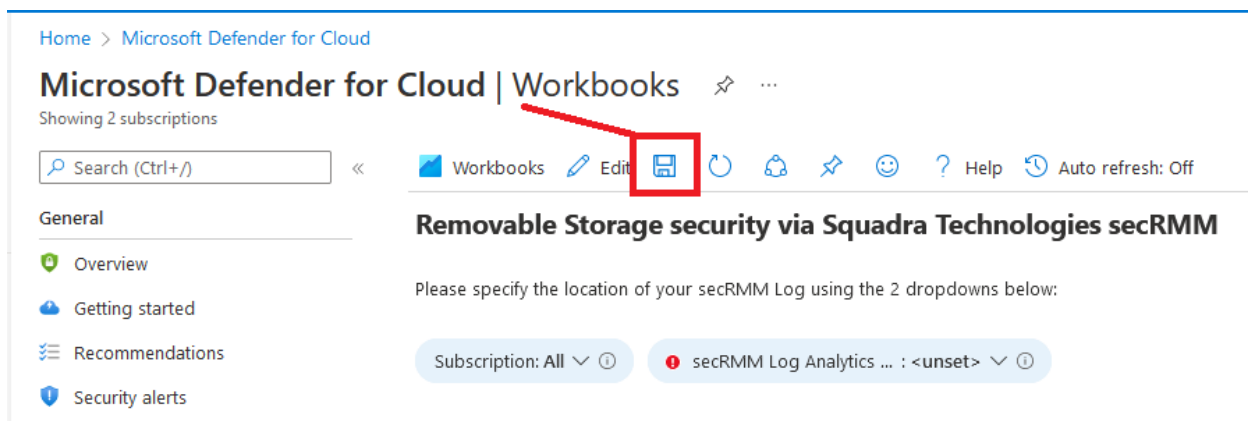
You can name the workbook anything you like.
We suggest naming it the same name as the file where you copied the json from.
Currently, the list of secRMM Azure Monitor Workbooks is:

secRMM Administration Events Azure.workbook
secRMM All Events Azure.workbook
secRMM Authorization Failure Events Azure.workbook
secRMM Device Events Azure.workbook
secRMM Online_Offline Events Azure.workbook
secRMM RemovableMedia By Encryption Azure.workbook
secRMM RemovableMedia By Model Azure.workbook
secRMM RemovableMedia By User Azure.workbook
secRMM Write Events Azure.workbook

Azure will save the workbook and you will get a notification as shown in the screenshot below.
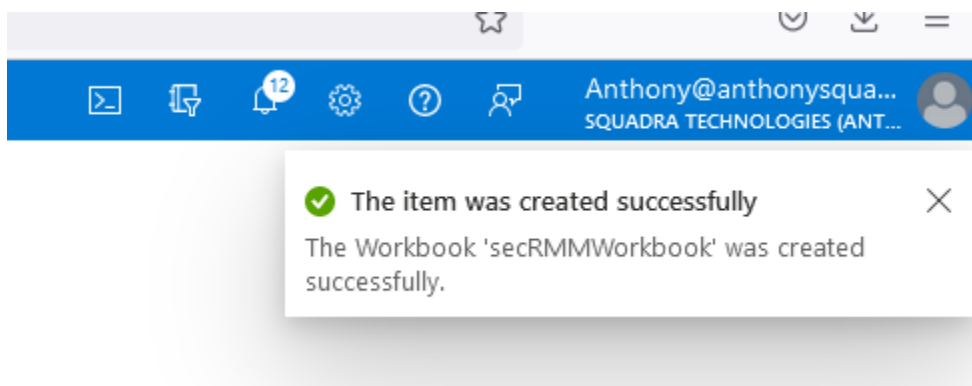
Now, if you click the workbooks button as shown in the screenshot below.
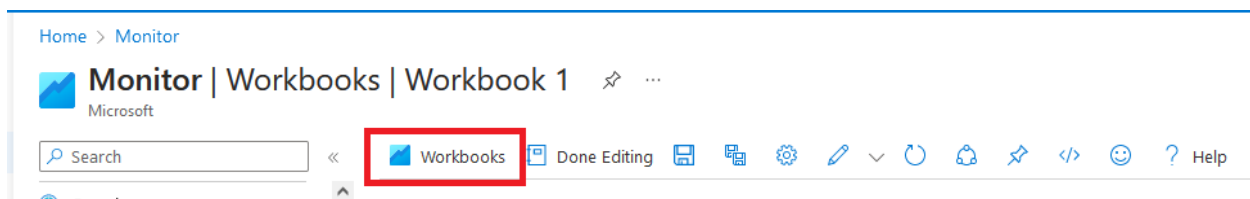
You will now see the secRMM Workbooks in the collection of Azure Monitor workbooks as shown in the screenshot below. Note that there seems to be a bug in this page where you will need to click the 'Reset Filters' link before the secRMM Workbooks.
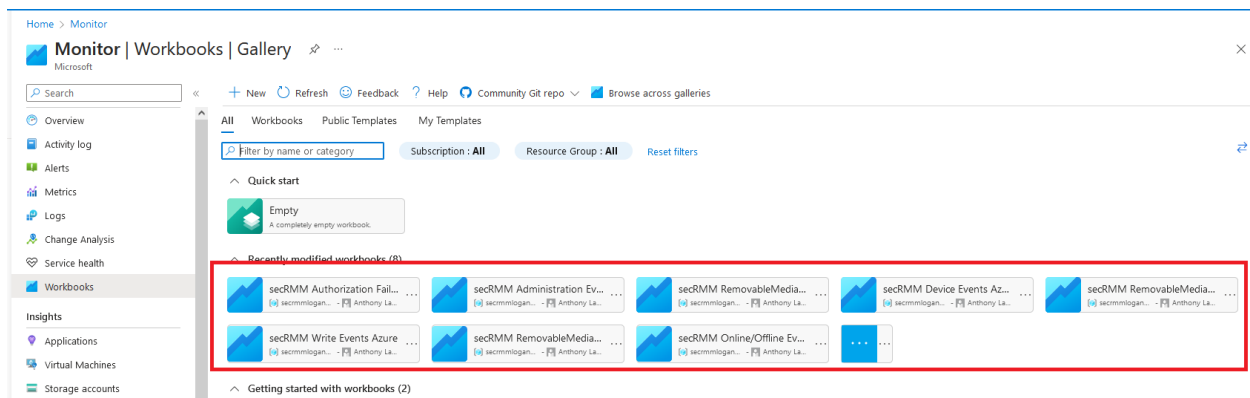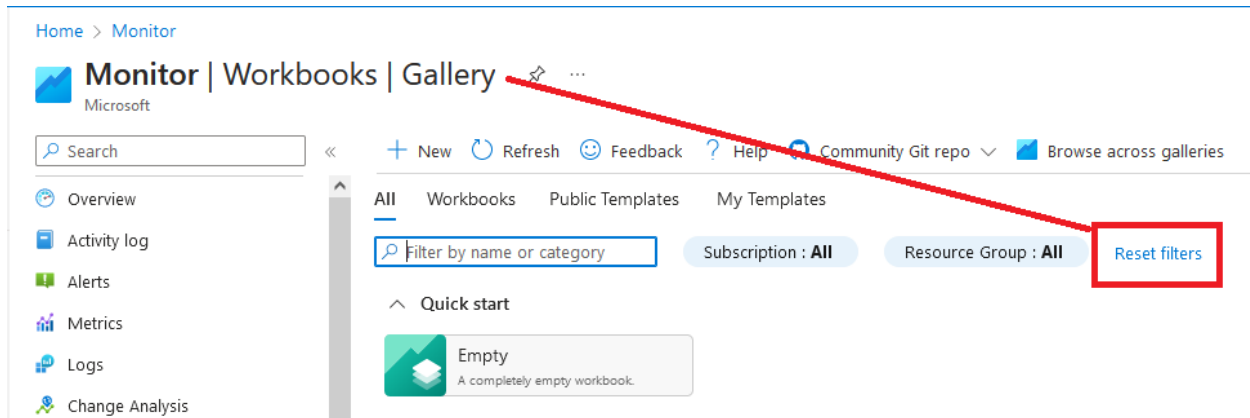
If you notice the secRMM Workbooks, the last box is an empty square, if you click it, it will show the workbooks in a list.
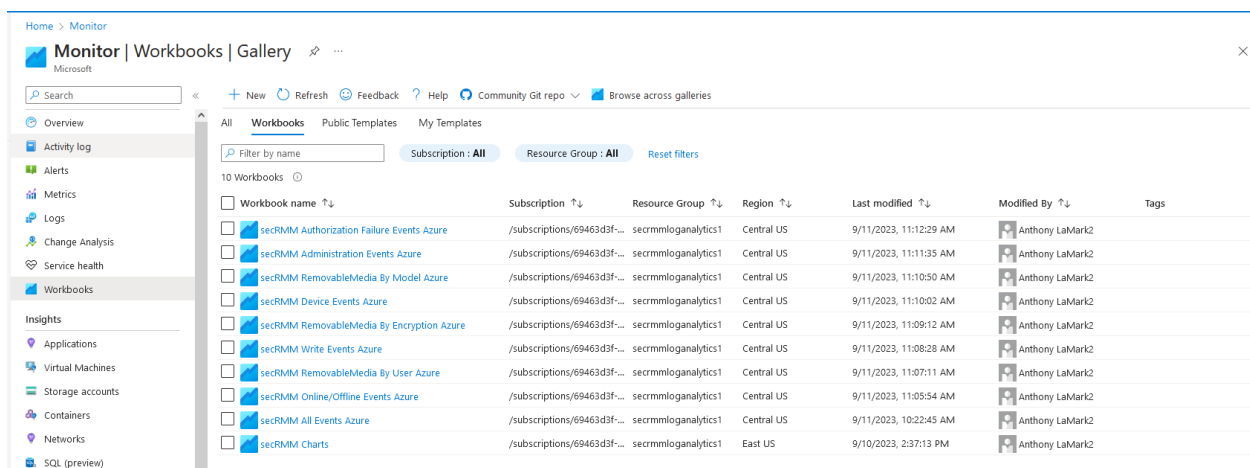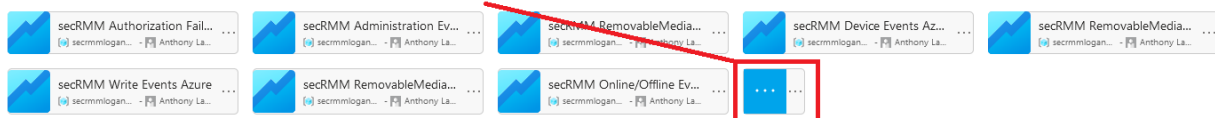
Connect "Azure Log Workspace for secRMM" to Azure Monitor

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

Click one of the "secRMM Azure Monitor workbooks" you just created as shown in the screenshot below.
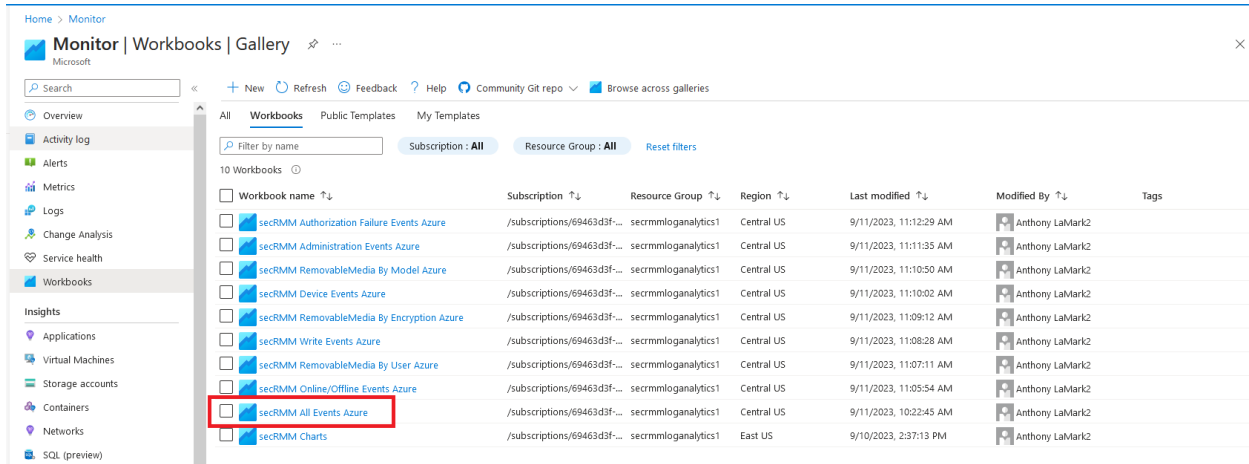
Click the 'LogAnalytics' drop-down as shown in the screenshot below.
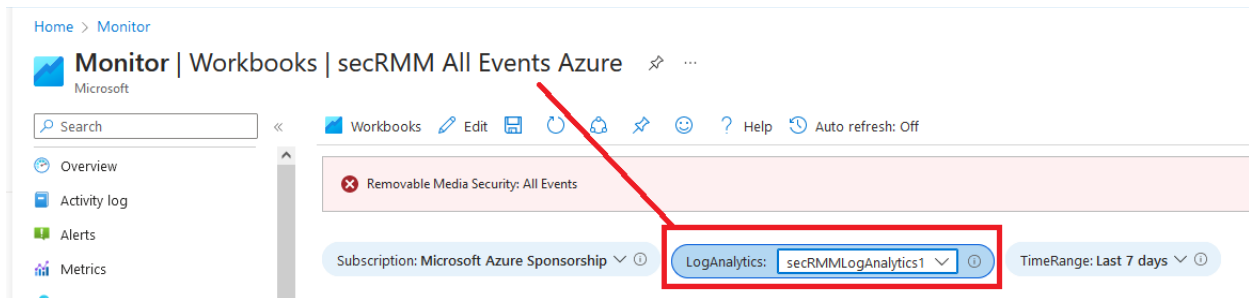
In the drop-down list, you will see the 'Azure Log Workspace for secRMM' as shown in the screenshot below (note that the name of your workspace will be different from the name in the screenshot below).
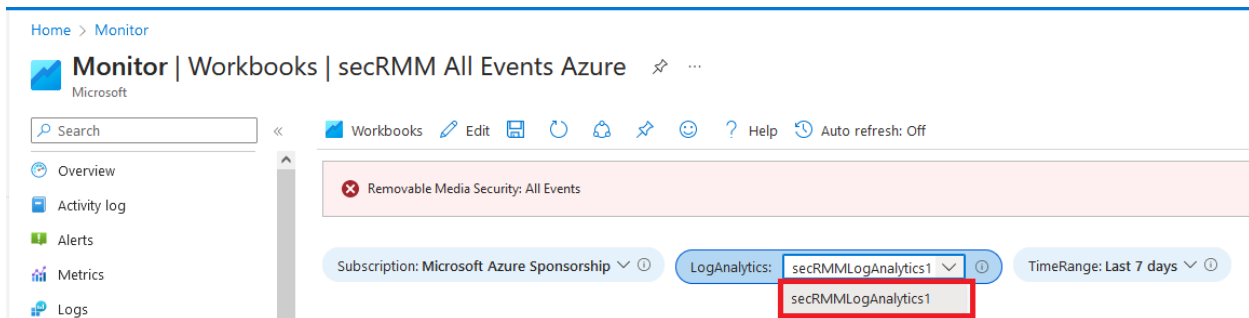
Once you select the workspace, the workbook will be ready to render the security events generated by secRMM. The next section shows how to tell secRMM to send the security events to the 'Azure Log Workspace'.

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.

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).
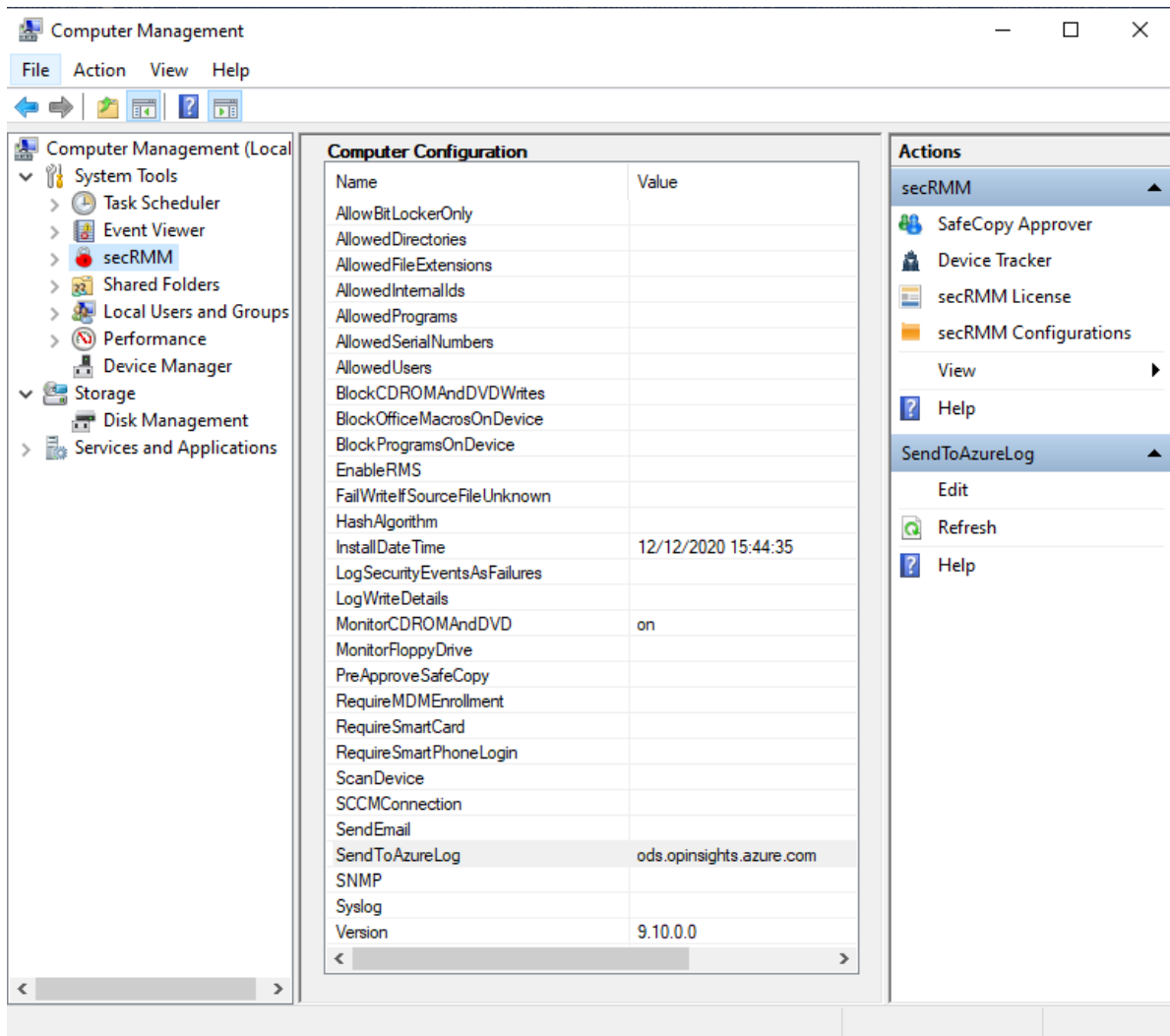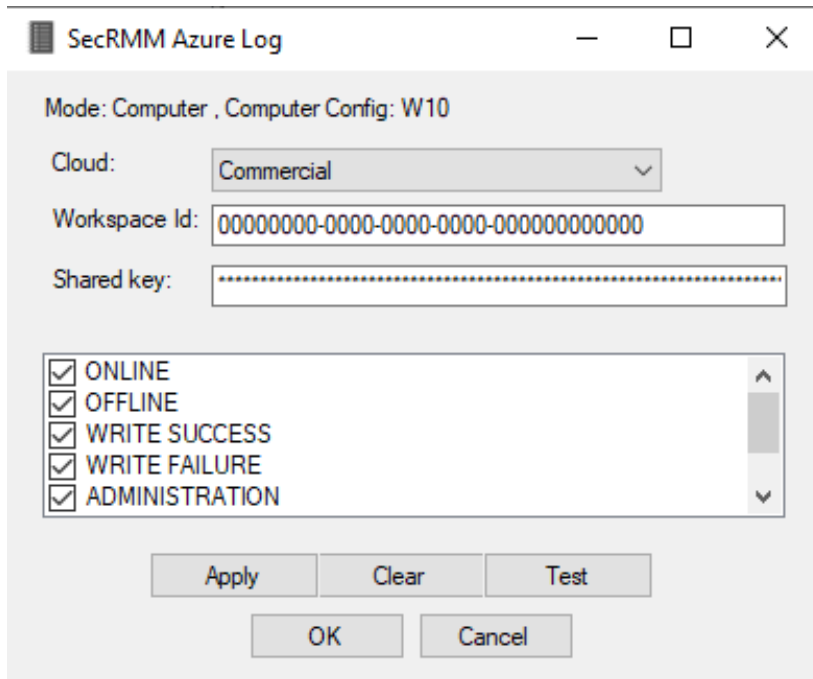
Specify the **WORKSPACE ID** and **PRIMARY KEY** that you copied when you created the "Log Analytics Workspace" in the subsection above titled *Create "Azure Log Workspace for secRMM"* into the secRMM

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.

Click the **Apply** button and then the **Test** button. If the test succeeds, you will see the Message box as shown below.
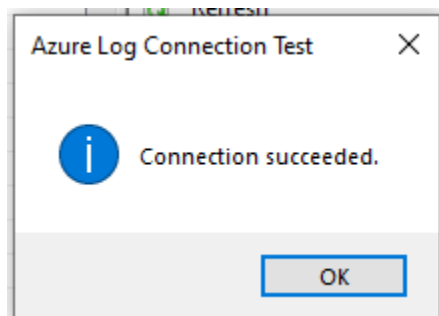
You can now use Azure Monitor to integrate your USB security into your overall security strategy!

Usage

Now that the secRMM security events are going into Azure Log Analytics and Azure Monitor, we can tell Azure Monitor 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 Monitor instance. If you want help setting up your removable storage security strategy, please feel free to contact Squadra Technologies support (support@squadratechnologies.com).

Azure Monitor 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	4C530010606231106322
Model	SanDisk Cruzer Glide USB Device
Internal Id	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_GLIDE&REV_1.00\4C530010606231106322&0
Program Name	"E:\HOLD\RunMe.cmd"
Additional Info	Command Line: E:\HOLD

secRMM Event Viewer: localhost, event log secRMM — Row: 11

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	4C530010606231106322
Model	SanDisk Cruzer Glide USB Device
Internal Id	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_GLIDE&REV_1.00\4C530010606231106322&0

secRMM Event Viewer: localhost, event log secRMM — Row: 5

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"))

secRMM Event Viewer: localhost, event log secRMM	— □ ✕

Row: 6   [Previous]   [Next]

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 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"))

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.

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

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
	7575 West Washington Ave. Suite 127-252
	Las Vegas, NV 89128
	USA

Web site   http://www.squadratechnologies.com/