Security Removable Media Manager
connector to
Azure Sentinel
Version 9.9.22.0
(January 2020)
Protect your valuable data
## Contents

**INTRODUCTION** ......................................................................................................................................... 4

- **DESCRIPTION** ................................................................................................................................. 4
- **WHY INTEGRATE secRMM SECURITY EVENTS INTO AZURE SENTINEL?** ........................................ 5

**CONFIGURATION** ................................................................................................................................... 5

- **PREREQUISITES** .............................................................................................................................. 5
- **CREATE “AZURE LOG WORKSPACE FOR secRMM”** ......................................................................... 6
- **CONNECT “AZURE LOG WORKSPACE FOR secRMM” TO AZURE SENTINEL** ............................... 11
- **CONFIGURE secRMM TO SEND EVENTS TO “AZURE LOG WORKSPACE FOR secRMM”** ................ 12

**USAGE** .................................................................................................................................................. 14

- **AZURE SENTINEL QUERIES** ............................................................................................................ 14
  - **Sample query 1 – ONLINE events** .................................................................................................... 15
  - **Sample query 2 – Count the number of failed write attempts events** ............................................. 15
  - **Sample query 3 – Which users are writing files to removable storage devices** ............................... 16
  - **More sample queries** .................................................................................................................... 17
    - Microsoft BitLocker Activity for removable storage devices ............................................................. 17
    - Microsoft Windows Defender Activity for removable storage devices ............................................. 17
    - Hardware Encrypted Device Activity ............................................................................................... 18
    - Users who have tried to execute macros or programs from a removable storage device .................. 18
    - Removable storage devices that are not encrypted (hardware or software) ...................................... 19
    - Removable storage devices that are mounted into a Virtual Machine ............................................ 20
      - Event on the physical machine ........................................................................................................ 20
      - Event on the virtual machine ........................................................................................................... 20
    - Show mobile devices that are being USB mounted ......................................................................... 20
    - Show mobile devices that are being USB mounted but are not MDM (Microsoft Intune) enrolled .... 21
- **AZURE SENTINEL WORKBOOK** ........................................................................................................ 21
- **AZURE SENTINEL ANALYTICS** ....................................................................................................... 22
- **AZURE LOG ANALYTICS secRMM SCHEMA** .................................................................................. 28
  - **Descriptions** ................................................................................................................................... 28

**CONTACTING SQUADRA TECHNOLOGIES SUPPORT** ........................................................................... 29

**ABOUT SQUADRA TECHNOLOGIES, LLC** ............................................................................................ 30
Introduction

Description

Azure 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 Azure 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 Azure Sentinel instance. This allows you 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 Azure Sentinel" to refer to this secRMM to Microsoft Azure 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 Azure 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 Azure 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) incidents and introductions of malware into a computing environment.

Configuration
Prerequisites

To use the "secRMM Connector to Microsoft Azure 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) 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 “Advanced Settings” 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.
Connect “Azure Log Workspace for secRMM” to Azure Sentinel

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

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

Click the Add 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).

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, AD GPO or locally in “Computer Management” console) will depend
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, 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 Sentinel to integrated your USB security into your overall security strategy!

**Usage**

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

**Azure 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 to 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
```
More sample queries

Microsoft BitLocker Activity for removable storage devices

secRMM_CL | where DeviceDescription_s contains "ENCRYPTED BitLocker"

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 Azure Sentinel Administrator Guide

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

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

```sql
secRMM_CL | where ((Event_s == "ONLINE") and (DeviceDescription_s !contains "ENCRYPTED"))
```
Removable storage devices that are mounted into a Virtual Machine

Event on the physical machine

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

![SecRMM Event Viewer: localhost, event log secRMM](image1)

Event on the virtual machine

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

![SecRMM Event Viewer: localhost, event log secRMM](image2)

Show mobile devices that are being USB mounted

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

![SecRMM Event Viewer: localhost, event log secRMM](image3)
Show mobile devices that are being USB mounted but are not MDM (Microsoft Intune) enrolled

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

**Azure Sentinel Workbook**

You can create an “Azure Sentinel Workbook” to see graphs and charts of the removable storage security events.
There is currently no method to import a workbook into your Azure 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

Azure Sentinel Analytics

This section will use “Azure Sentinel Analytics” to make your “Azure 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 Azure 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).
Click the “Create” link and then select the “Scheduled 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 screenshot below).
Rule creation wizard

General  Set rule logic  Automated response  Review and create

Create an analytic rule that will run on your data to detect threats.

Analytic rule details

Name *
 Removable Storage ONLINE

Description
 Detect when a removable storage device is plugged in by the end-user.

Tactics

Discovery

Severity

High

Status

Enabled  Disabled

Next : Set rule logic >
Put the following query into the “Rule query” text field in the next form and then click the “Next : Automated response” button (as shown in the screenshot below).

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

**Map entities - more entities coming soon!**

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string or Datetime.

<table>
<thead>
<tr>
<th>Entity Type</th>
<th>Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>Defined in query</td>
</tr>
<tr>
<td>Host</td>
<td>Defined in query</td>
</tr>
<tr>
<td>IP</td>
<td>Choose column</td>
</tr>
</tbody>
</table>
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.

- **AdditionalProgramInfo_s**: Additional program information (used in cmd.exe, powershell, vbscript and jscript programs).
- **Computer**:
- **ConfigurationTarget_s**:
- **DeviceDescription_s**:
- **Drive_s**: SourceFileLastWrite_s
- **Event_s**: SourceFileSize_s
- **InternalID_s**: SourceFile_s
- **ManagementGroupName**: SourceSystem
- **Message**: TargetFile_s
- **Model_s**: TimeGenerated
- **PreviousPropertyValue_s**: Time_s
- **ProgramName_s**: Type
- **ProgramPID_s**: UserSID_s
- **PropertyAction_s**: User_s
- **PropertyName_s**: Volume_s

**Descriptions**
| **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/