

Security Removable Media Manager connector to

# **Azure Monitor**

Version 9.11.27.0 (April 2024) 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 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

# Contents

INTRODUCTION	4
	4
WHY INTEGRATE SECRMM SECURITY EVENTS INTO AZURE MONITOR?	4
CONFIGURATION	5
Prerequisites	5
CREATE "AZURE LOG WORKSPACE FOR SECRMM"	5
DOWNLOAD AND IMPORT THE 'SECRMM AZURE MONITOR WORKBOOKS'	
CONNECT "AZURE LOG WORKSPACE FOR SECRMM" TO AZURE MONITOR	
CONFIGURE SECRMM TO SEND EVENTS TO "AZURE LOG WORKSPACE FOR SECRMM"	19
USAGE	20
Azure Monitor Queries	21
Sample query 1 – ONLINE events	
Sample query 2 – Count the number of failed write attempts events	
Sample query 3 – Which users are writing files to removable storage devices	
Sample query 4 – Which users attempted writing files to removable storage devices but failed	
More sample queries	
Microsoft BitLocker Activity for removable storage devices	22
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
Azure Log Analytics secRMM schema	
Descriptions	
CONTACTING SQUADRA TECHNOLOGIES SUPPORT	
ABOUT SQUADRA TECHNOLOGIES, LLC.	

# 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:

<u>http://www.squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx</u>, 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).

A Ho	me - Microso	ft Azure	×	+		
$\leftarrow \rightarrow$	C 🗘	🗎 po	rtal.azure	.com/#ho	ome	
Арр	s 📙 STC	STS	, Tech	nology	, Personal	
Micro	soft Azure					
» +				Az	ure servi	ces
<b>^</b>					+	
=					Create a resource	Log Analytics workspaces

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

🔥 Log	g Analytics wo	orkspaces - Micro 🗙	+	
$\leftarrow \rightarrow$	C 🗅	portal.azure.co	om/#blade/HubsEx	tension/Brc
Арр	os 📙 STC	📙 STS 🔄 Techno	ology 📙 Personal	
Micro	soft Azure			
>>	Home >	Log Analytics workspac	ces	
+	Log An Squadra Tech	alytics workspac	ces	
	+ Add	=≡ Edit columns 🐧	)Refresh 🛛 🖉 🖉	Assign tags
=	Subscript	ions: Visual Studio Ent	erprise: BizSpark	
- * -	Filter by r	iame		All r
◆	1 items	ie ↑↓	Resource g	ıroup ↑↓

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.

🔥 Lo	g Analytics workspace - Micros 🗙 🕂
$\leftarrow \rightarrow$	C 🗅 portal.azure.com/#create/Microsoft.LogAnaly
App	os 🚺 STC 🛄 STS 📜 Technology 🛄 Personal
Micro	osoft Azure
>>	Home > Log Analytics workspaces > Log Analytics workspace
+	Log Analytics workspace $\Box$ ×
	Create New      Link Existing
=	Log Analytics Workspace * ()
- *	Subscription *
٠	Visual Studio Enterprise: BizSpark 🗸
æ	Resource group *
	Logs 🗸
	Create new
	Location *
0	West US 🗸

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

🔥 Log	Analytics workspaces - Micro 🗙 🕂
$\leftarrow \rightarrow$	C 🏠 🏽 portal.azure.com/#blade/HubsExtension/BrowseResourceBlade/reso
App	s 📕 STC 📑 STS 📑 Technology 📑 Personal
Micro	soft Azure
»	Home > Log Analytics workspaces
+	Log Analytics workspaces Squadra Technologies
1	+ Add ≡≡ Edit columns 💍 Refresh 🛛 🔗 Assign tags
	Subscriptions: Visual Studio Enterprise: BizSpark
- *	secRMMSecurityEvents All resource groups
	1 items
Ē	Name $\uparrow_{\downarrow}$ Resource group $\uparrow_{\downarrow}$
	secRMMSecurityEvents Logs

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.

	▲ Advanced settings - Microsoft A: × +				
<del>\</del>	→ C 1 Portal.azure.com/#@ar	thonysqu	adratechnologies.onmicrosoft.com/	resource/subscriptic	ons/3fbb9579-25a7-4188-ac10-e544a9aedfde/resourceGroups/Logs/providers/Mi
Ap	ops 📙 STC 📕 STS 📕 Technology 📕	Personal			
Micr	osoft Azure			𝒫 Search resource	s, services, and docs (G+/)
*	Home > Log Analytics workspaces > sec	RMMSecur	ityEvents > Advanced settings		
+	Advanced settings				
	🕐 Refresh 🛛 🗜 Logs				
	(?) Connected Sources	>	📒 Windows Servers	>	Windows Servers Attach any Windows server or client.
-×	🖉 Data	>	👌 Linux Servers	>	0 WINDOWS COMPUTERS CONNECTED Download Windows Agent (64 bit)
	Computer Groups	>	Azure Storage	>	Download Windows Agent (32 bit) You'll need the Workspace ID and Key to install the agent.
			े System Center	>	WORKSPACE ID fc6b6e96-d5ba-4dc9-92f1-77c39b3a6fb2
					PRIMARY KEY
<b>♦</b>					iyru1xRZ8z/AGIYyJMV38ra8mrNodE8Ug6DI

# Download and import the 'secRMM Azure Monitor Workbooks'

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

Home >> secRMM >> Downloads >> System Center/Azure >> Azure Monitor

secRMM Azure Monitor Integration		
Azure Monitor allows you to incorporat	te 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 Azure Munitor.		
Item	Download link	
secRMM Azure Monitor Workbooks	secRMMAzureWorkbooks.zip	

Clicking the 'secRMMAzureWorkbooks.zip' link will download the workbooks to your downloads folder as shown in the screenshot below.

onprovid	organize
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\blacklozenge$ > This P	C → Downloads
<ul> <li>Quick access</li> <li>secRMM</li> <li>Downloads</li> <li>Documents</li> </ul>	Name Vesterday (1) secRMMAzureWorkbooks.zip
📥 OneDrive - Personal	
This DC	

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.

Home >
Monitor   Overview
<mark>,                                    </mark>
Overview
Activity log
💶 Alerts
👬 Metrics
P Logs
🐥 Change Analysis
⊗ Service health
🞽 Workbooks
Insights

On the 'Monitor | Workbooks | Gallery' page, click the 'Empty' workbook as shown in the screenshot below.

O Search	🗌 « 🔪 🕂 New 💍 Refresh 😳 Feedback  ? Help  🖓 Community Git repo 🗸 🎽 Browse across galleri
Overview	Workbooks Public Templates My Templates
Activity log	Patter by name or category Subscription : All Resource Group : All Reset filters
Alerts	
Metrics	
Logs	Empty
Change Analysis	
Service health	<ul> <li>Recently modified workbooks (0)</li> </ul>
Workbooks	No items found.
	<ul> <li>Getting started with workbooks (2)</li> </ul>

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

Home > Monitor	
Monitor   Wo	rkbooks   Workbook 1 🖈 …
Microsoft	
♀ Search	🛛 🐇 🦉 Workbooks 📳 Done Editing 🔚 🖷 🎯 🖉 🗸 🗘 😂 🖈 🛷 😳 🤶 Help
🕑 Overview	
Activity log	This Workbook has no content.
💵 Alerts	
艏 Metrics	Use the add button below to add items.
🧬 Logs	+ Add >z
🐥 Change Analysis	
💝 Service health	
🧹 Workbooks	

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

Home > Monitor	
Monitor   Workbo	ooks   Workbook 1 🖈 …
₽ Search	« 🎽 Workbooks 🛽 Done Editing 🔚 🖷 🕸 🖉 🗸 🖒 🍰 🖈 🕩 😳 🤶 Help
🕑 Overview	Shown below is a JSON representation of the current item.
Activity log	Any changes you make here will be reflected when you press 'Apply'.
💵 Alerts	Template Type ①
🖬 Metrics	Gallery Template ARM Template
🧬 Logs	<pre>{     "version": "Notebook/1.0". </pre>
🐥 Change Analysis	"items": [], Remove this.
℅ Service health	"Azure Monitor"
Workbooks	], "\$schema": "https://github.com/Microsoft/Application-Insights-Workbooks/blob/master/schema/workbook.json"
Insights	

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.

🎽 Workbooks 🗉 Done Editing 🔚 🖷 🐵 🖉 🗸 🏷 🕼 🖈 🕫 🔅 🥇 Help



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

Home > Microsoft Defender for Cloud		
Microsoft Defender for Showing 2 subscriptions	Cloud   Workbooks 🛷 …	×
	🎽 Workbooks 🖻 Done Editing 🔚 😼 🎯 🖉 🗸 🖒 🖾 🖈 🕩 🎯 ? Help	
General	Removable Storage security via Squadra Technologies secRMM	^
Overview		↑ Edit ····
<ul> <li>Getting started</li> </ul>		
š≡ Recommendations	Please specify the location of your secRMM Log using the 2 dropdowns below:	t Edit
Security alerts		- Edit
🤫 Inventory	Externition All V 0 • restable los tendetirs V 0	
🧹 Workbooks	Subscription: All Y 🔍 🔮 Sectionine Log Anlangues , Cutiser Y 🐨	
4 Community		↑ Edit ····
Diagnose and solve problems		

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

Home > Microsoft Defender for Cloud							
Microsoft Defender for Cloud   Workbooks 🖉 … Showing 2 subscriptions							
	👅 Workbooks 🖉 Edit 🔚 💍 🍰 🖈 😳 🤶 Help 🕚 Auto refresh: Off						
General	Removable Storage security via Squadra Technologies secRMM						
Overview							
😃 Getting started	Please specify the location of your secRMM Log using the 2 dropdowns below:						
3 Recommendations	Subscription: All 🗸 ① 🛛 😝 secRMM Log Analytics : < unset > 🗸 ①						
Security alerts							

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 RemovableMedia By User 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.

nome / womitor		
Monitor   W	Vorkbooks   Gallery 🟒 …	
Microsoft		
₽ Search	🛛 🚽 👋 👋 👋 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉	owse across galleries
🕑 Overview	All Workbooks Public Templates My Templates	_
Activity log	P Filter by name or category Subscription : All Resource Group : All	Reset filters
💶 Alerts		A contract of the second secon
Metrics	∧ Quick start	
₽ Loas	Empty	
	A completely empty workbook.	
🐥 Change Analysis		
Home > Monitor <b>Monitor</b>   Workbooks   €	Gallery 🖈 …	
A Search +	- New 🚺 Refrech 😳 Feerlhark 2 Heln 🖸 Community Git reno 🗸 🧃 Browse arross nalleries	
Overview	Workbooks Public Templates My Templates	
Activity log	Filter by name or category Subscription : All Resource Group : All Reset filters	
Activity log	Fitter by name or category         Subscription : All         Resource Group : All         Reset filters           Outlet start	
Activity log	Filter by name or category         Subscription : All         Resource Group : All         Reset filters           Quick start	
Activity log  Alerts  Metrics  Constraints	Filter by name or category     Subscription : All     Resource Group : All     Reset filters       Quick start     Empty A complex workbook.     Filter by not book.	
Activity log Activity log Activity log Activity log Activity log Activity log Control Activi	Filter by name or category     Subscription : All     Resource Group : All     Reset filters       Quick start       Imply     A complexity workbook.	
Activity log Activity log Activity log Activity log Activity log Activity log Control Activity log Activity	Filter by name or category     Subscription : All     Resource Group : All     Reset filters       Quick start       Empty       A complexity workbook.	
Activity log Acti		secRMM RemovableMedia
Activity log Acti	Filter by name or category       Subscription : All       Resource Group : All       Reset filters         Quick start       Empty       A complexity workbook.         SecRMM Authorization Fail	secRMM RemovableMedia joj seconticgan 19 Actiony La.
Activity log Activity log Alerts Activity log Activity log Activity log Activity log Activity log Activity log Comparison Compariso	Subscription : All       Resource Group : All       Reset filters         Quick start       Subscription : All       Reset filters         Empty       A complexity workbook.       Subscription : All       Reset filters         SecRMM Authorization Fail	secRMM RemovableMedia )oj secremicgan 1¶ Actiony La.
Activity log Activity log Alerts Alerts Construction Con	Filter by name or category       Subscription : All       Resource Group : All       Reset filters         Quick start       Subscription : All       Reset filters         Marcon Support Sup	secRMM RemovableMedia (a) seconocyta (P) Antony La.

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.

secRMM Authorizatio	n Fail secRMM Administration Ev hony La · M Anthony La ·	seckivi M.R. (ii) secriming	emovableMedia anthrp=thony_ta	se	RMM Device Events Az	secRMM Re [9] secrmmloga	emovableMedia	
secRMM Write Events	S Azure SecRMM RemovableMedia	secRMM C (*) secrmmlag	Dnline/Offline Ev an M Anthony La_		]			
Home > Monitor								
<mark>Monitor</mark>   Workbo	ooks   Gallery 🖉 …							$\times$
Microsoft		in channa 🖉 ba						
>> Search	Refresh C Feedback / Help C Con	mmunity Git repo 🗸 🧧 Bro	wse across galleries					
) Overview	All Workbooks Public Templates My Templates							
Activity log	Filter by name Subscription : All	Resource Group : All	Reset filters					
Alerts	10 Workbooks ①							
á Metrics	Workbook name ↑↓	Subscription ↑↓	Resource Group ↑↓	Region ↑↓	Last modified ↑↓	Modified By ↑↓	Tags	
Logs	secRMM Authorization Failure Events Azure	/subscriptions/69463d3f	secrmmloganalytics1	Central US	9/11/2023. 11:12:29 AM	Anthony LaMark2		
Change Analysis	SecRMM Administration Events Azure	/subscriptions/69463d3f	secrmmloganalytics1	Central US	9/11/2023. 11:11:35 AM	Anthony LaMark2		
Service health	SecRMM RemovableMedia By Model Azure	/subscriptions/69463d3f	secrmmloganalytics1	Central US	9/11/2023. 11:10:50 AM	Anthony LaMark2		
Workbooks	serBMM Device Events Azure	/subscriptions/69463d3f-	secromloganalytics1	Central US	9/11/2023 11:10:02 AM	Anthony LaMark2		
hts	serBMM BemovableMedia By Encryption Azure	/subscriptions/69463d3f	secromloganalytics1	Central US	9/11/2023 11:09:12 AM	Anthony LaMark2		
pplications	section removable view by Encryption Azure	/subscriptions/69463d3f-	secromloganalytics1	Central US	9/11/2023 11:08:28 AM	Anthony LaMark2		
Virtual Machines		/subscriptions/69463d3f-	secromloganalytics1	Central US	9/11/2022 11:07:11 AM	Anthony Lakdark2		
Storage accounts		/subscriptions/69463d3f	secromloganalytics1	Central US	9/11/2023 11:05:54 AM	Anthony Lakdark2		
Containers	Concentration of the events Addree	/subscriptions/69463d3f-	secromloganalytics1	Central US	9/11/2023 10:22:45 AM	Anthony Lakdark2		
Networks	Secrements Azure	/subscriptions/60462-d24-	secromloganalytics1	Fact LIS	0/10/2023 2:37:13 DM	Anthony LaMark2		
5 SQL (preview)	Section of the company of the compan	, subscriptions/05403031	scanningalialytics	Last ob	5/10/2020, 201113 PW	Anthony Edividi K2		

## 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.

Here & Meriker						
Monitor   Workboo	ks   Gallery 🖈 …					×
₽ Search «	+ New 💍 Refresh 🐵 Feedback 🤉 Help 🌻 Con	nmunity Git repo 🗸 🎽 Browse across galleries				
Overview	All Workbooks Public Templates My Templates					
Activity log	P Filter by name Subscription : All	Resource Group : All Reset filters				
💵 Alerts	10 Workbooks ③					
Metrics	Workbook name ↑↓	Subscription ↑↓ Resource Group ↑↓	. Region ↑↓	Last modified ↑↓	Modified By ↑↓	Tags
🧬 Logs	secRMM Authorization Failure Events Azure	/subscriptions/69463d3f secrmmloganalytics1	Central US	9/11/2023, 11:12:29 AM	Anthony LaMark2	
🐥 Change Analysis	SecRMM Administration Events Azure	/subscriptions/69463d3f secrmmloganalytics1	Central US	9/11/2023. 11:11:35 AM	Anthony LaMark2	
💝 Service health	Contraction of the second seco	/subscriptions/60462d2fserrmmloganalities1	Control LIS	9/11/2022 11/10/50 AM	Anthony LaMark2	
🞽 Workbooks		/subscriptions/69462d2fa serromloganalytics	Central US	9/11/2023, 11:10:02 AM	Anthony Labiark2	
Insights	sectivity Device Events Azure	/subscriptions/69463d3f sectrimingganalytics	Central US	0/11/2023, 11:00:12 AM	Anthony Latviark2	
Applications	seckimik kemovablemedia by Encryption Azure	/subscriptions/69463d3i* Secriminoganalytics	Central US	9/11/2023, 11:09:12 AM	Anthony Lawark2	
Virtual Machines	seckMM Write Events Azure	/subscriptions/69463d3t secrmmioganalytics i	Central US	9/11/2023, 11:08:28 AM	Anthony LaMark2	
	SecRMM RemovableMedia By User Azure	/subscriptions/69463d3t secrmmloganalytics1	Central US	9/11/2023, 11:07:11 AM	Anthony LaMark2	
storage accounts	secRMM Online/Offline Events Azure	/subscriptions/69463d3f secrmmloganalytics1	Central US	9/11/2023, 11:05:54 AM	Anthony LaMark2	
de Containers	secRMM All Events Azure	/subscriptions/69463d3f secrmmloganalytics1	Central US	9/11/2023, 10:22:45 AM	Anthony LaMark2	
Networks	secRMM Charts	/subscriptions/69463d3f secrmmloganalytics1	East US	9/10/2023, 2:37:13 PM	Anthony LaMark2	
🗟 SQL (preview)						

Click the 'LogAnalytics' drop-down as shown in the screenshot below.

Home > Monitor		
📈 Monitor   Workb	ooks	secRMM All Events Azure 🖉 \cdots
Microsoft		
₽ Search	«	🎽 Workbooks 🖉 Edit 🔚 💛 👶 🖈 😳 🤶 Help 🕄 Auto refresh: Off
Overview	^	
Activity log		Kemovable Media Security: All Events
💵 Alerts		
m Metrics		Subscription: Microsoft Azure Sponsorship $\checkmark$ 0 LogAnalytics: secRMMLogAnalytics1 $\checkmark$ 0 TimeRange: Last 7 days $\checkmark$ 0

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).

Home > Monitor						
Monitor   Workb	oks   secR	MM All Events A	\zure ☆	·		
₽ Search	« 🧹 Workb	ooks 🖉 Edit 🔚 💍	ا م	🙂 🤶 Help	🕚 Auto refresh: Off	
Overview						
Activity log	Kem	ovable Media Security: All Ever	ts			
💵 Alerts						
🖬 Metrics	Subscript	tion: Microsoft Azure Spons	orship $\vee$ $\odot$	LogAnalytics:	secRMMLogAnalytics1 🗸 🕕	TimeRange: Last 7 days $\checkmark$ ①
₽ Logs					secRMMLogAnalytics1	

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 (<u>support@squadratechnologies.com</u>) 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).

🜆 Computer Management			- 🗆 X
File Action View Help			
· · · · · · · · · · · · · · · · · · ·			
🜆 Computer Management (Local	Computer Configuration		Actions
✓ <sup>™</sup>	Name	Value	secRMM
> 🕗 Task Scheduler	AllowBitLockerOnly		
> 🛃 Event Viewer	AllowedDirectories		85 SafeCopy Approver
> 🧉 secRMM	AllowedFileExtensions		A Device Tracker
> 就 Shared Folders	AllowedInternalIds		= secRMM License
> 🜆 Local Users and Groups	AllowedPrograms		sectivity License
> 🚳 Performance	AllowedSerialNumbers		secRMM Configurations
🛔 Device Manager	AllowedUsers		View 🕨
🗸 🚰 Storage	BlockCDROMAndDVDWrites		
Pisk Management	BlockOfficeMacrosOnDevice		Help
> 🛃 Services and Applications	Block ProgramsOn Device		SendToAzurel.og
	EnableRMS		
	FailWritelfSourceFileUnknown		Edit
	HashAlgorithm		Q Refresh
	InstallDateTime	12/12/2020 15:44:35	
	LogSecurityEventsAsFailures		Неір
	LogWriteDetails		
	MonitorCDROMAndDVD	on	
	MonitorFloppyDrive		
	PreApproveSafeCopy		
	RequireMDMEnrollment		
	RequireSmartCard		
	RequireSmartPhoneLogin		
	ScanDevice		
	SCCMConnection		
	SendEmail		
	SendToAzureLog	ods.opinsights.azure.com	
	SNMP		
	Sysiog	0.10.0.0	
	version	9.10.0.0	
	< .	>	
< >			

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 Azu	ire Log	_		Х
Mode: Computer	, Computer Config: W10			
Cloud:	Commercial		$\sim$	
Workspace Id:	0000000-0000-0000-0000-000	00000000	0	
Shared key:				•••••
ONLINE OFFLINE WRITE SUC WRITE FAIL ADMINISTR	CCESS LURE ATION Apply Clear OK Cancel	Test		<b>`</b>

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

Azure Log Connection Test	×
Connection succeeded.	
ОК	

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 (<u>support@squadratechnologies.com</u>).

### **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"

interpretation in the second seco

Row	β2	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"))

📴 se	ecRMM Eve	nt Viewer: localhost, event log secRMM -		$\times$
Row	<b>r</b> : β8	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 fo	und no thre	ats.

#### 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\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\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\_CL | where ((Event\_s == "BLOCK MACROS ON DEVICE ACTIVE") or (Event\_s == "BLOCK PROGRAMS ON DEVICE ACTIVE")) | summarize count() by User\_s

îr :	BecRMM 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		CONTOSO\Administrator	
	User SID	S-1-5-21-194330278-343332919-2867172138-500	
	Drive	E:	
Volume \Device\HarddiskVolume9		\Device\HarddiskVolume9	
Device Description Removable Disk Removable Media Win32_LogicalDisk USB2.0		Removable Disk Removable Media Win32_LogicalDisk USB2.0	
Serial Number 4C530001060623106322		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 Event Viewer: localhost, event log secRMM -		
R	ow: 5	Previous Next
	Name	Value
►	Event	ONLINE
	Time	01/01/2020 01:39:02 PM
Computer secRMMDemo1.CONTOSO.com		secRMMDemo1.CONTOSO.com
User CONTOSO\Administrator		CONTOSO\Administrator
	Drive	E:
Volume \Device\HarddiskVolume8		\Device\HarddiskVolume8
Device Description Removable Disk Removable Media Win32_LogicalDisk USB2.0		Removable Disk Removable Media Win32_LogicalDisk USB2.0
Serial Number 4C530001060623106322		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"))

📴 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 "^"))
```

📴 se	📴 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		DC.CONTOSO.com	
	User	CONTOSO\Administrator	
	Drive SECRMMDEMO1^E:		
	Volume \Device\HarddiskVolume8		
Device Description Removable Disk Removable Media Win32_LogicalDisk USB2.0		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"))

	Be secRMM Event Viewer: archive file X:\temp.evtx − □ >		
	Row: 8	Previous Next	
Γ	Name	Value	
٢	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-f98f491d4f3	33}
	Additional Info	MDM Info: Intune MDM Name: Anthony_Android_10/2/2019_5:54 PM(f2892637-6396-4bf0-9e91-4c2	34dc4

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

 $\times$ 

\_

secRMM\_CL | where ((Event\_s == "ONLINE") and (AdditionalProgramInfo\_s contains
"Mobile device is not MDM enrolled"))

BecRMM 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	<pre>t PropertyValue_s</pre>
t ConfigurationTarget_s	t RawData
t DeviceDescription_s	t SerialNumber_s
t Drive_s	<pre>t SourceFileLastWrite_s</pre>
t Event_s	t SourceFileSize_s
t InternalID_s	t SourceFile_s
t ManagementGroupName	t SourceSystem
t Message	<pre>t TargetFile_s</pre>
t Model_s	O TimeGenerated
t PreviousPropertyValue_s	t Time_s
t ProgramName_s	t Type
t ProgramPID_s	t UserSID_s
t PropertyAction_s	t User_s
<pre>t PropertyName_s</pre>	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 <u>http://www.squadratechnologies.com/</u>