



Security Removable Media Manager
connector to

Azure Sentinel

Version 9.11.27.0
(April 2024)

Protect your valuable data



secRMM Azure Sentinel 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

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	10
CONFIGURE secRMM TO SEND EVENTS TO “AZURE LOG WORKSPACE FOR secRMM”	11
USAGE	13
AZURE SENTINEL QUERIES	14
<i>Sample query 1 – ONLINE events.....</i>	<i>14</i>
<i>Sample query 2 – Count the number of failed write attempts events.....</i>	<i>14</i>
<i>Sample query 3 – Which users are writing files to removable storage devices</i>	<i>15</i>
<i>Sample query 4 – Which users attempted writing files to removable storage devices but failed.....</i>	<i>16</i>
<i>More sample queries.....</i>	<i>16</i>
Microsoft BitLocker Activity for removable storage devices	16
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
<i>Descriptions.....</i>	<i>28</i>
CONTACTING SQUADRA TECHNOLOGIES SUPPORT	29
ABOUT SQUADRA TECHNOLOGIES, LLC.....	30

secRMM Azure Sentinel Administrator Guide

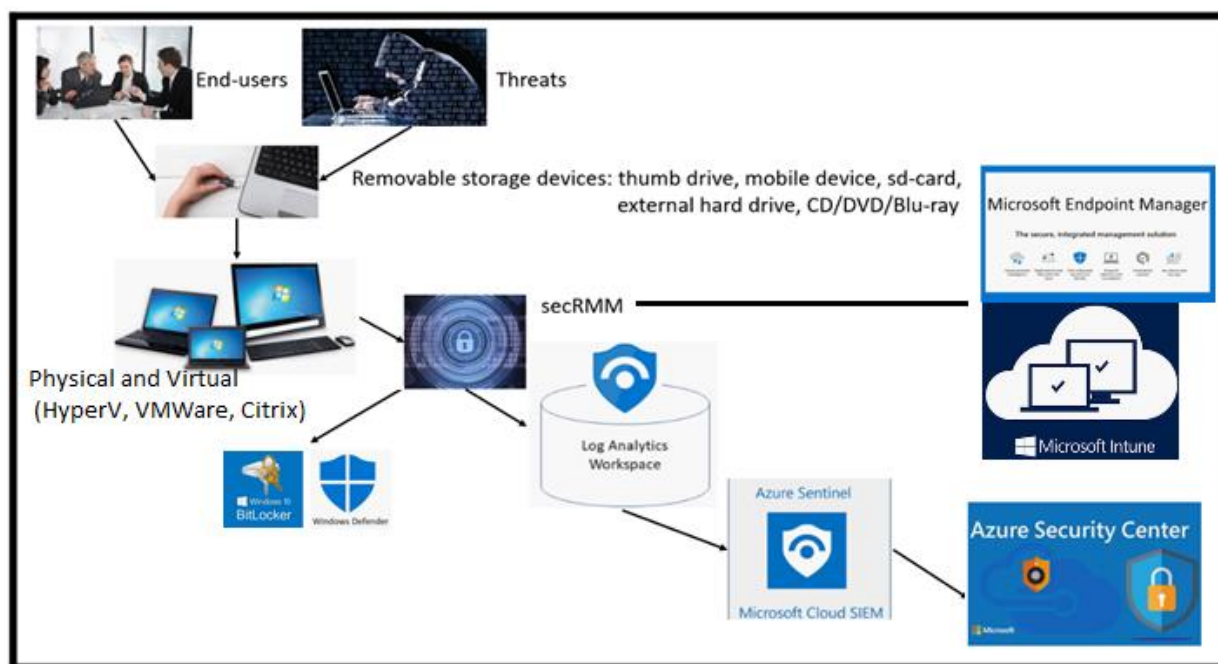
Introduction

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 to see the security events that secRMM generates within Sentinel. This architecture is diagramed below. Note that the Windows computers can be either on-premise or in the cloud.

The remainder of this document will use the term "secRMM Connector to Microsoft 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) /”Insider Threat Protection” (ITP) 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.

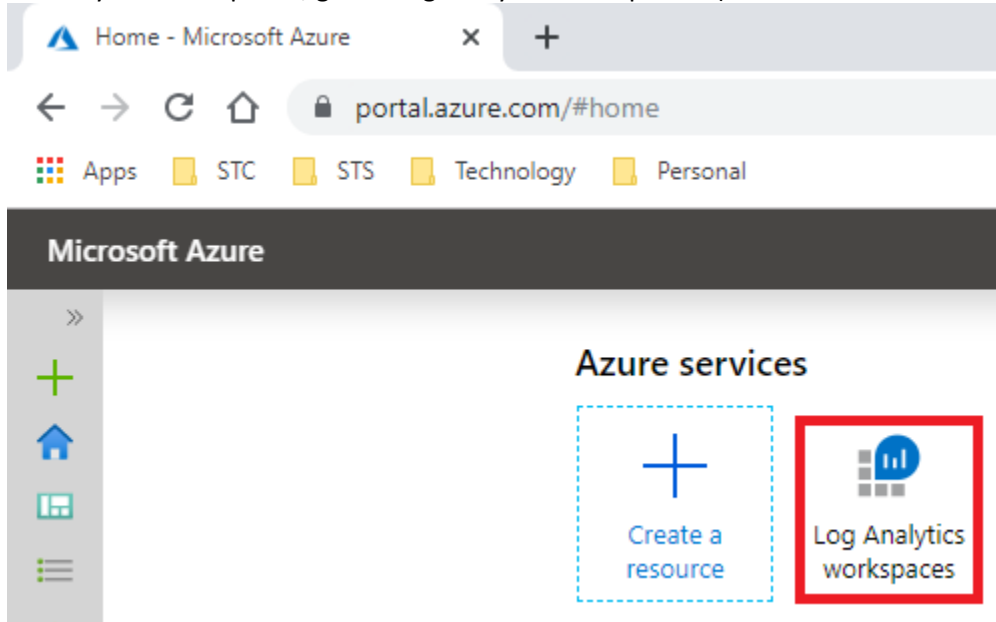
Deploying secRMM can occur using Active Directory, System Center Configuration Manager (SCCM), Intune or any other Windows software deployment tool. A secRMM deployment is a standard Windows MSI file installation. The documentation to deploy secRMM is on the Squadra Technologies web site at:

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

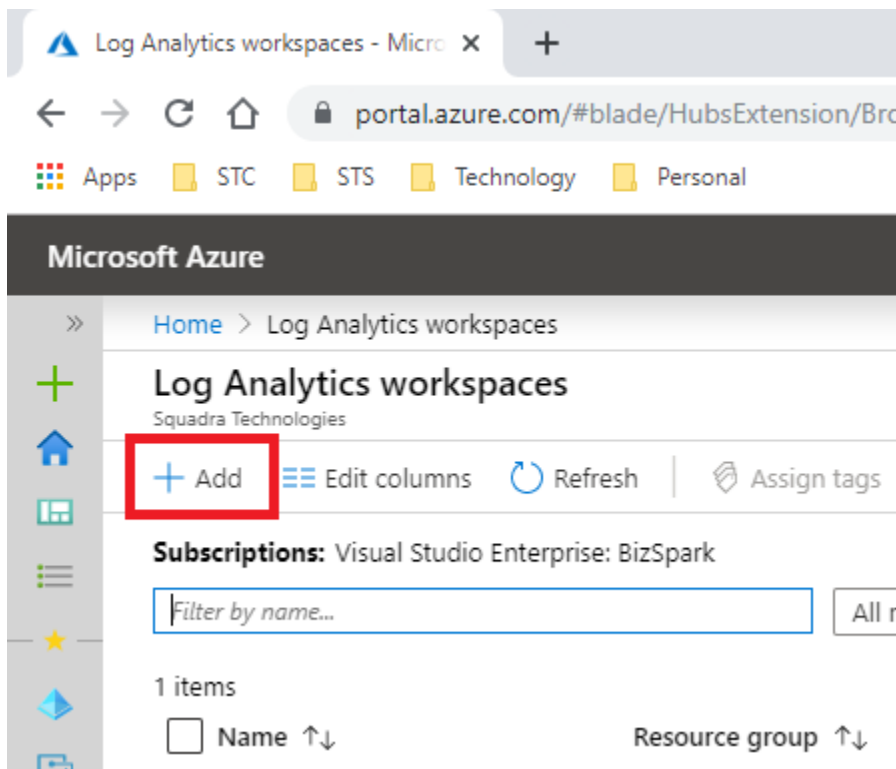


Create “Azure Log Workspace for secRMM”

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

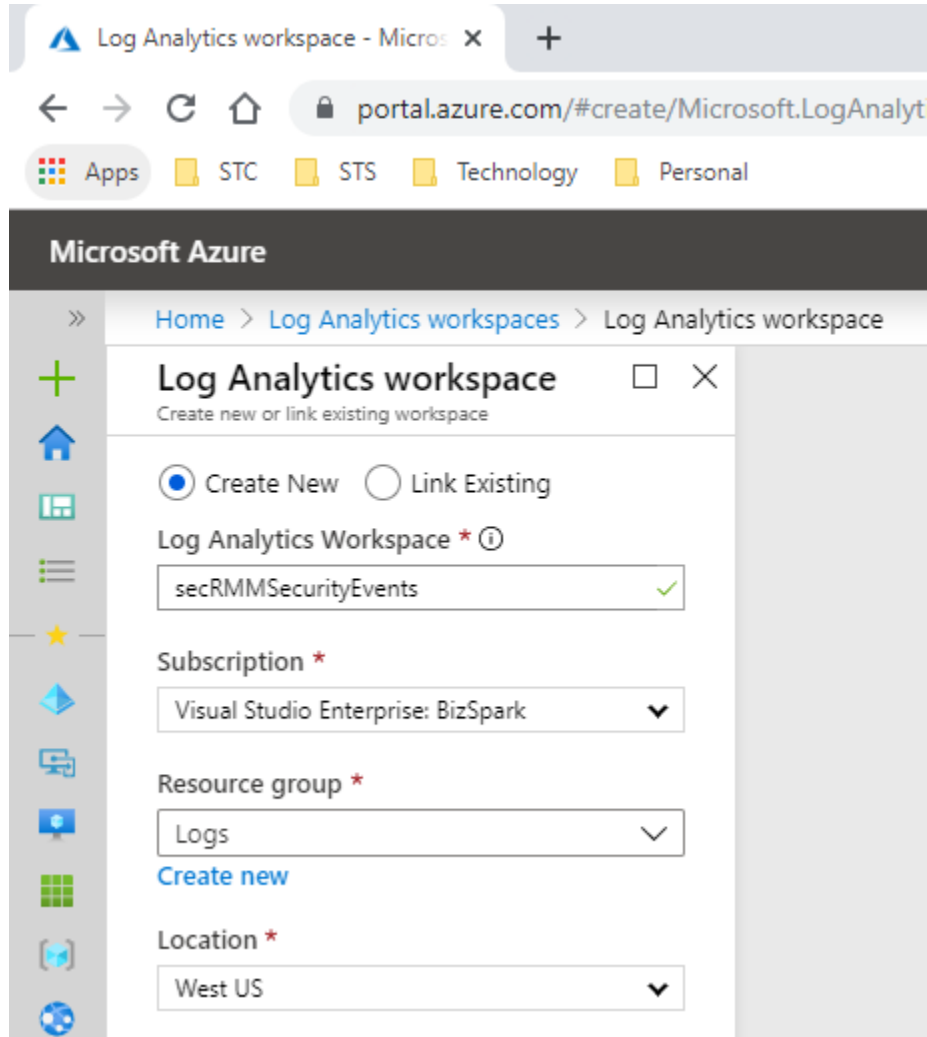


Within your Azure “Log Analytics workspaces”, click the Add link (as shown in the screenshot below).



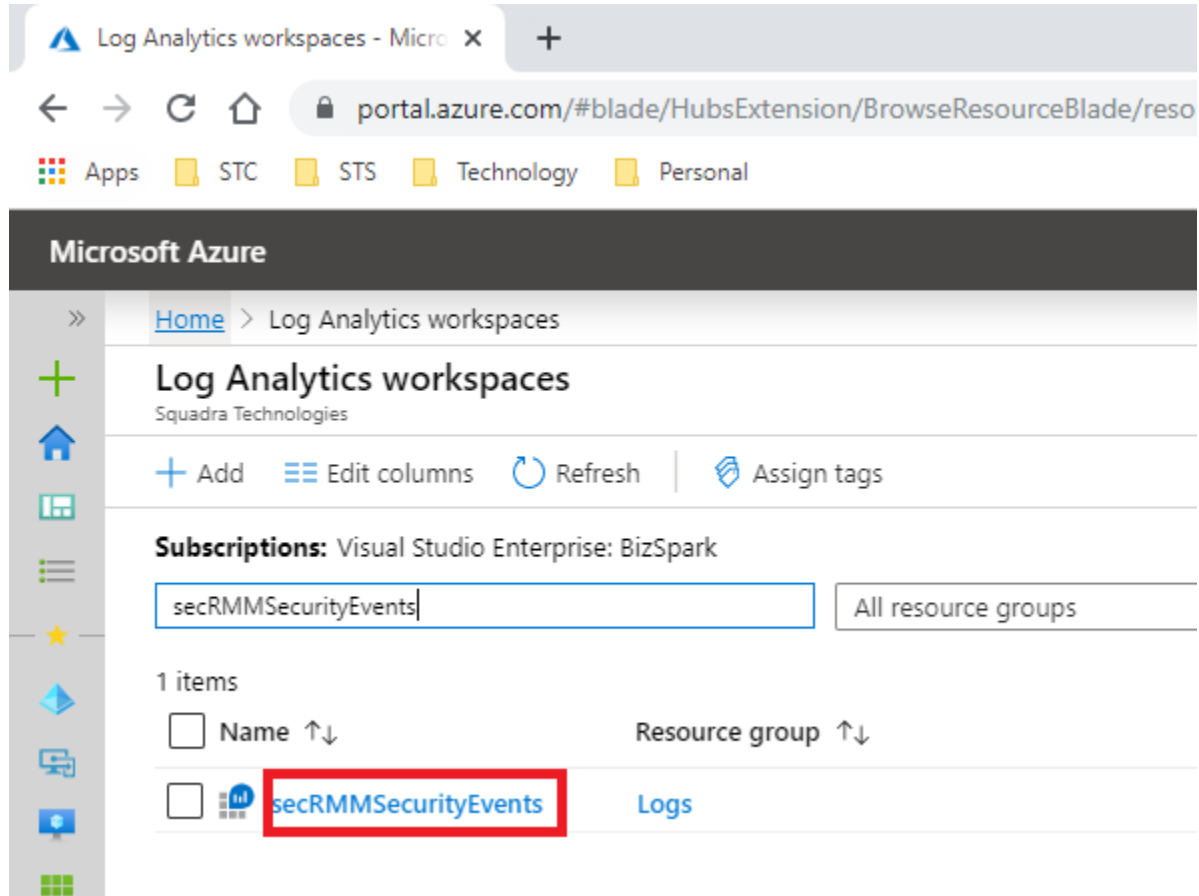
Fill out the form (as shown in the screenshot below).

Note that the values you specify here will be different based on your Azure environment.

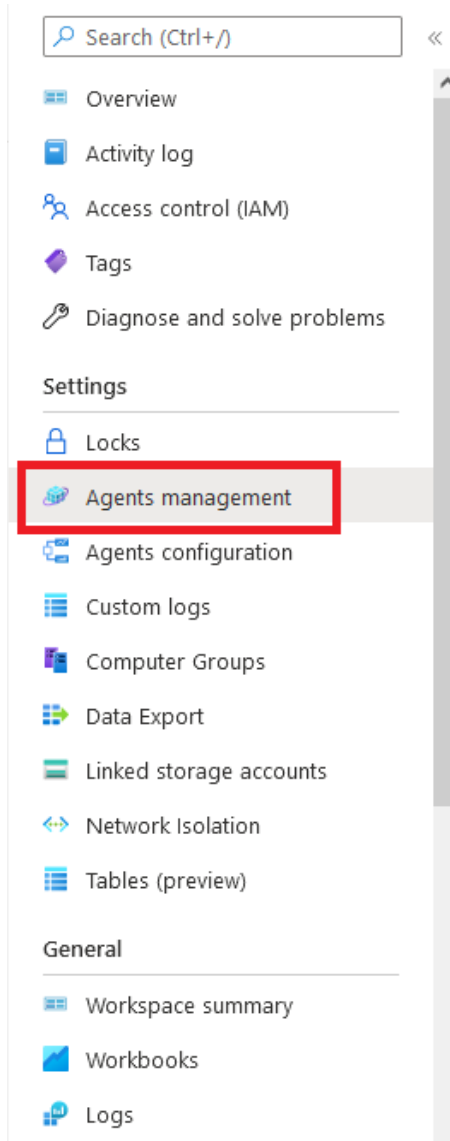


Once the “Log Analytics workspace” is created, click the name (as shown in the screenshot below).

secRMM Azure Sentinel Administrator Guide

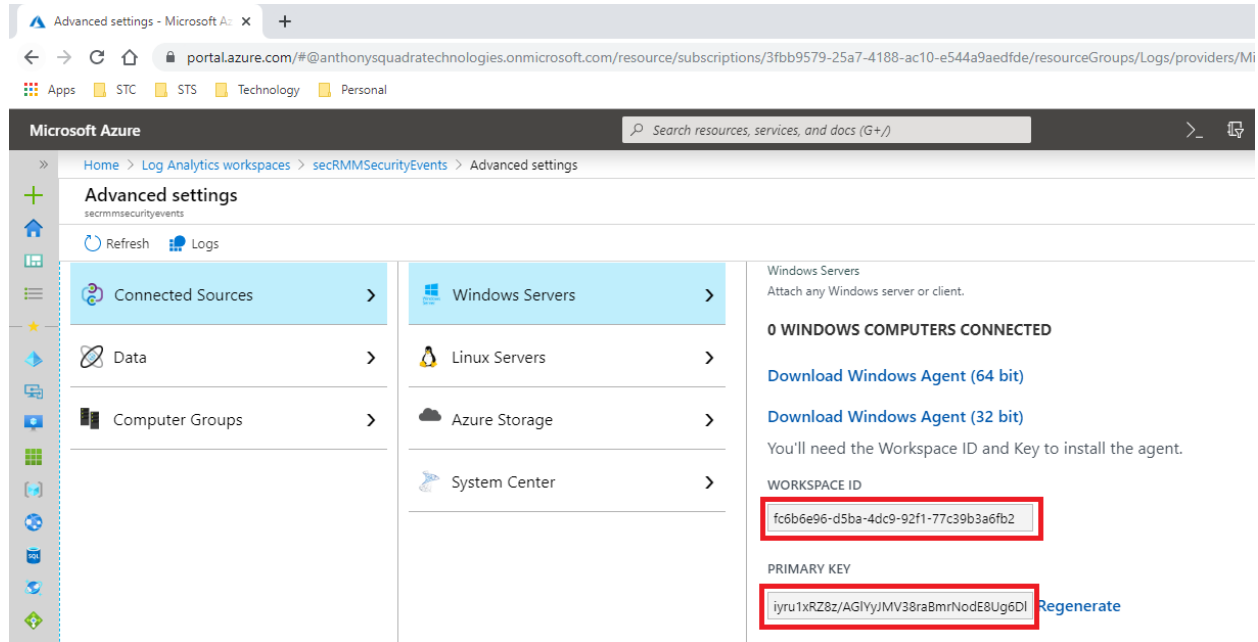


Click the “Agents management” link (as shown in the screenshot below).



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.

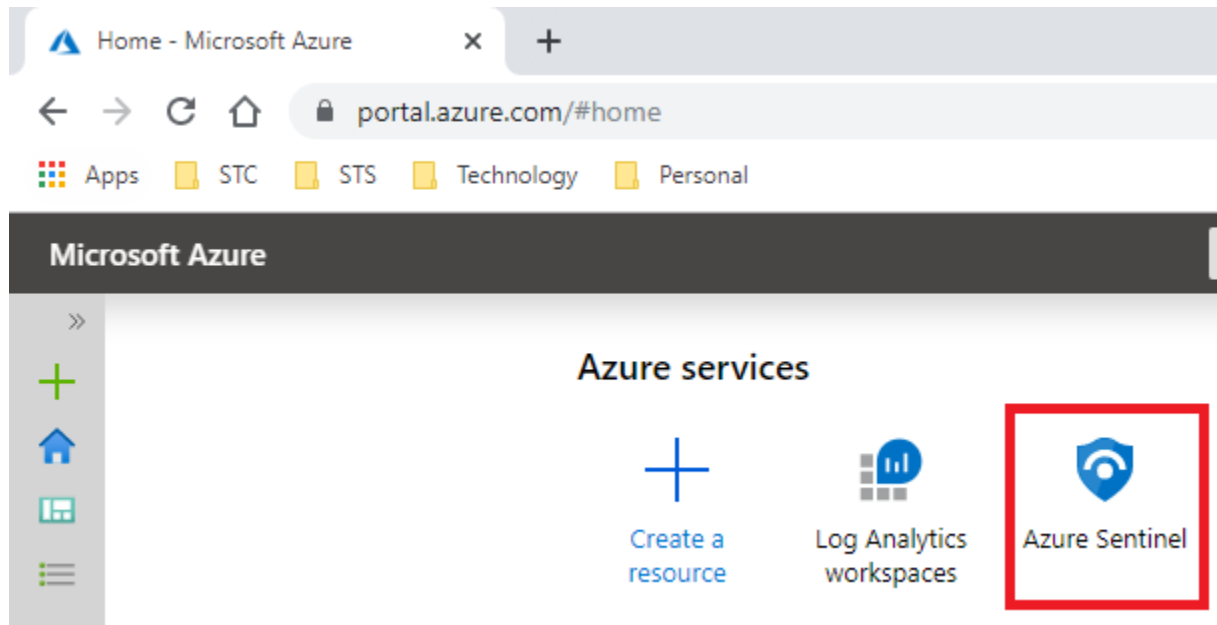
secRMM Azure Sentinel Administrator Guide



Connect “Azure Log Workspace for secRMM” to Azure Sentinel

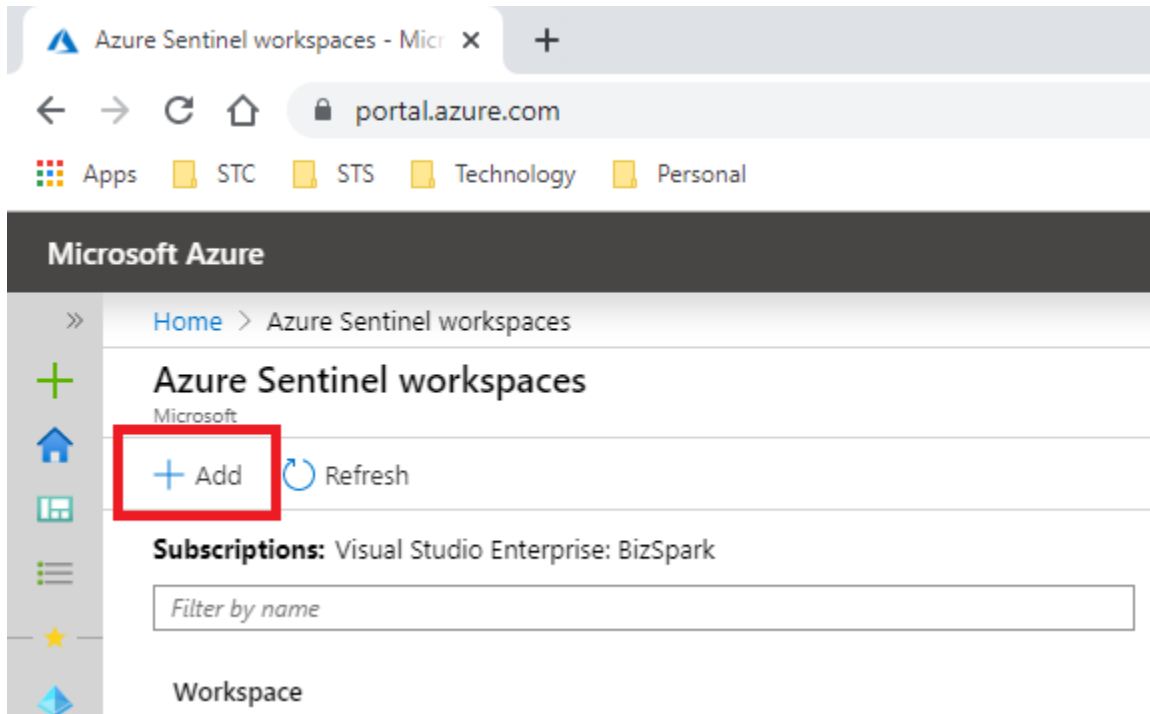
Now that you have created a “Azure Log Workspace for secRMM” (from the subsection above), you will connect the “Azure Log Workspace for secRMM” to your Azure Sentinel instance.

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

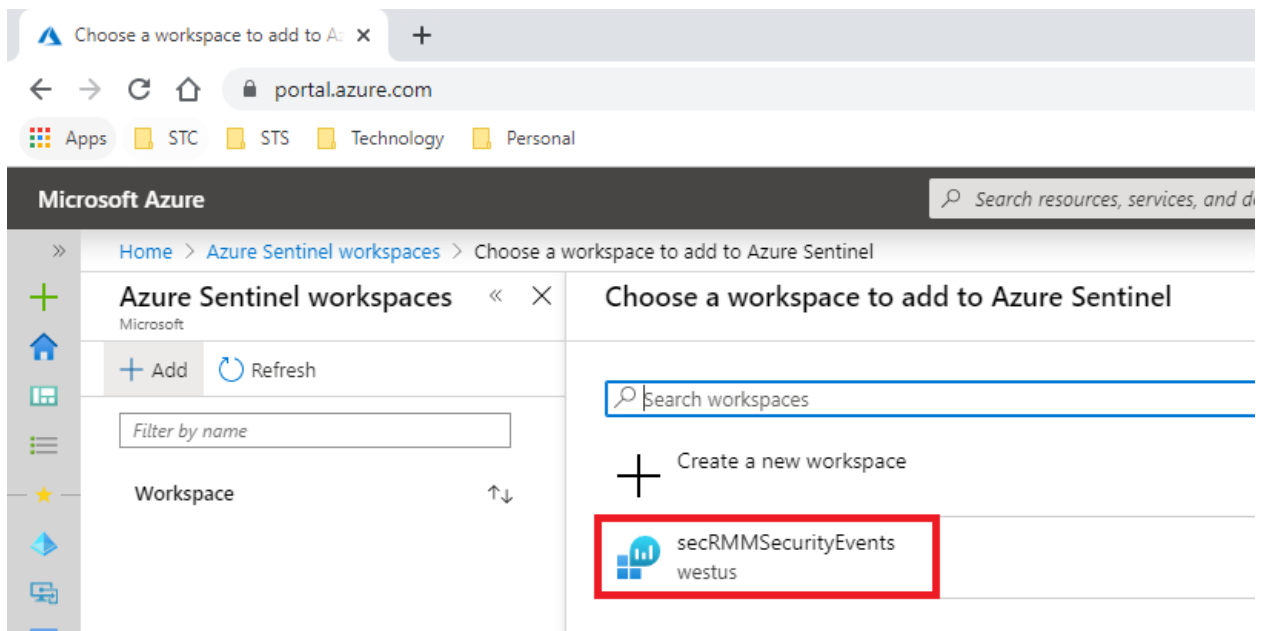


Click the Add link (as shown in the screenshot below).

secRMM Azure Sentinel Administrator Guide



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



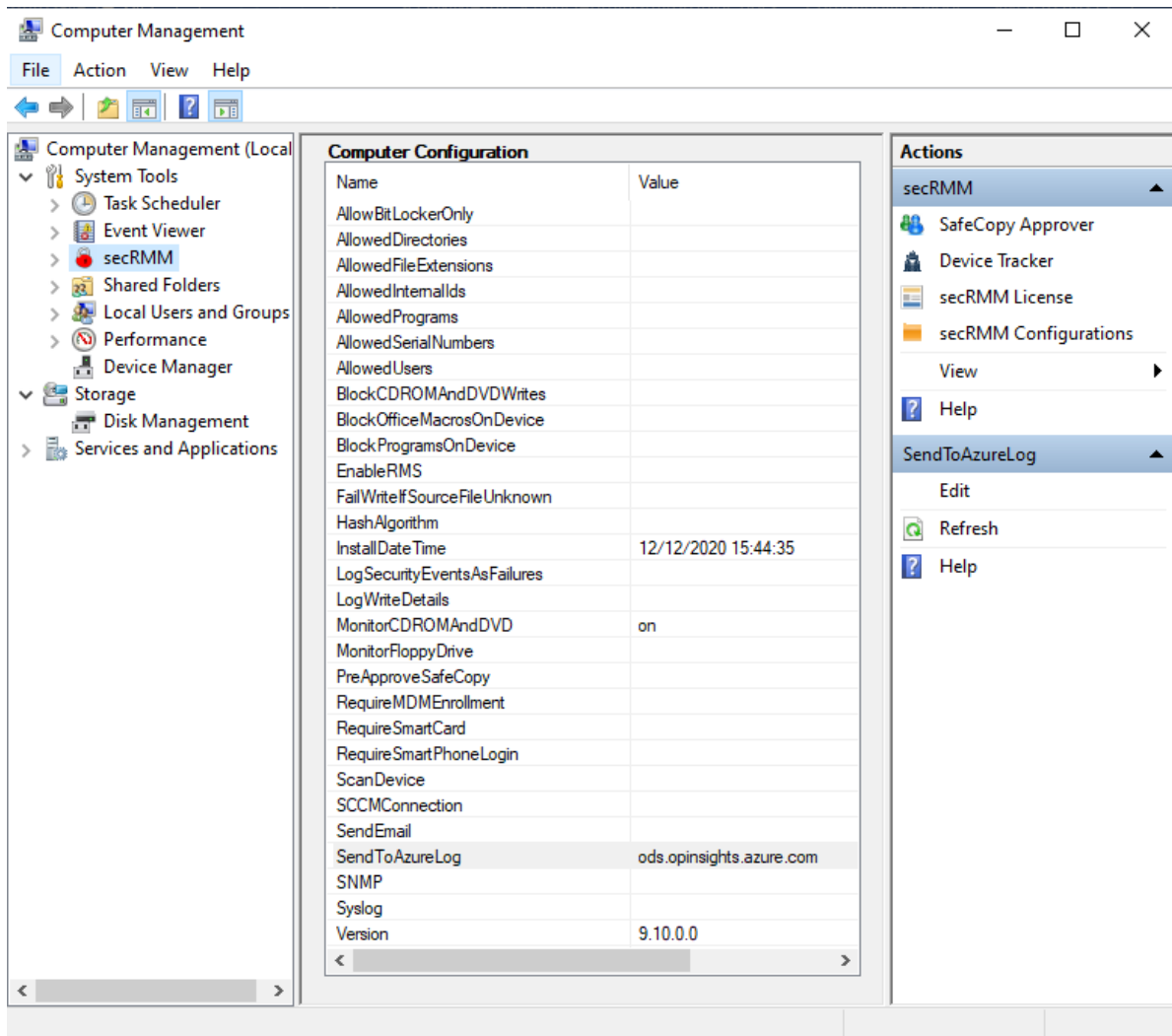
Configure secRMM to send events to “Azure Log Workspace for secRMM”

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, Intune, AD GPO or locally in “Computer Management” console) will

secRMM Azure Sentinel Administrator Guide

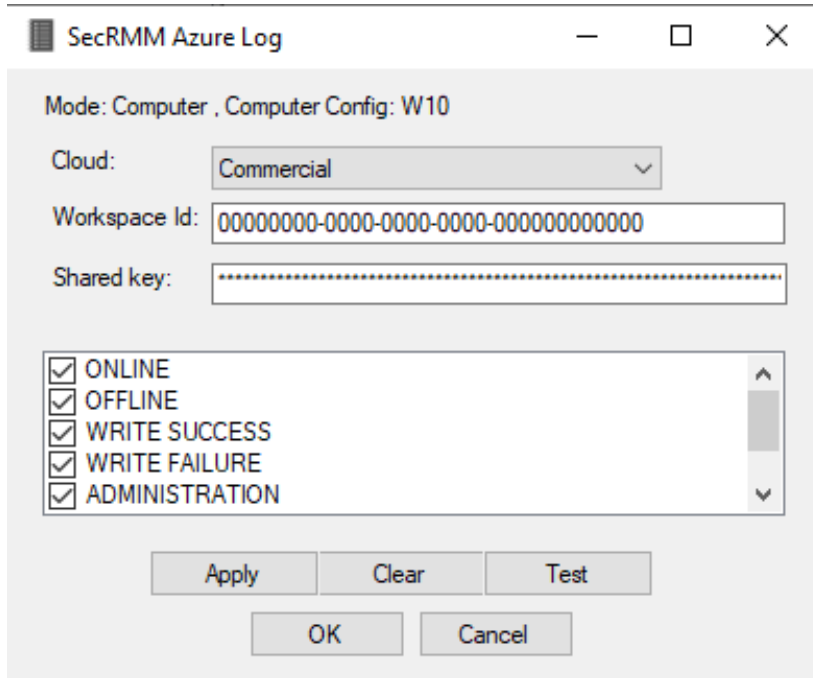
depend on how you are managing secRMM in your environment. If you are unsure, please just contact Squadra Technologies support (support@squadratechnologies.com) and we will help you with the setup.

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).



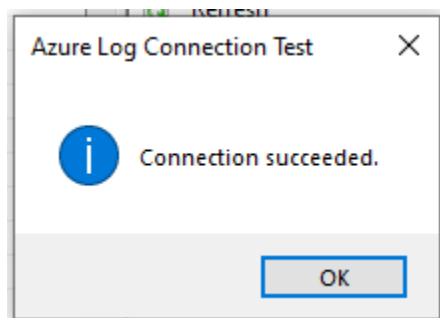
Specify the **WORKSPACE ID** and **PRIMARY KEY** that you copied when you created the “Log Analytics Workspace” in the subsection above titled *Create “Azure Log Workspace for secRMM”* into the secRMM dialog (as shown in the screenshot below). Note that the **PRIMARY KEY** is called “Shared key” in secRMM. 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.



The screenshot shows a window titled "SecRMM Azure Log". At the top, it says "Mode: Computer , Computer Config: W10". Below this, there are three input fields: "Cloud:" with a dropdown menu showing "Commercial", "Workspace Id:" with a text box containing "00000000-0000-0000-0000-000000000000", and "Shared key:" with a masked text box. Below these fields is a list of checkboxes, all of which are checked: "ONLINE", "OFFLINE", "WRITE SUCCESS", "WRITE FAILURE", and "ADMINISTRATION". At the bottom of the window are five buttons: "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 Sentinel 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 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).

secRMM Azure Sentinel Administrator Guide

Azure Sentinel Queries

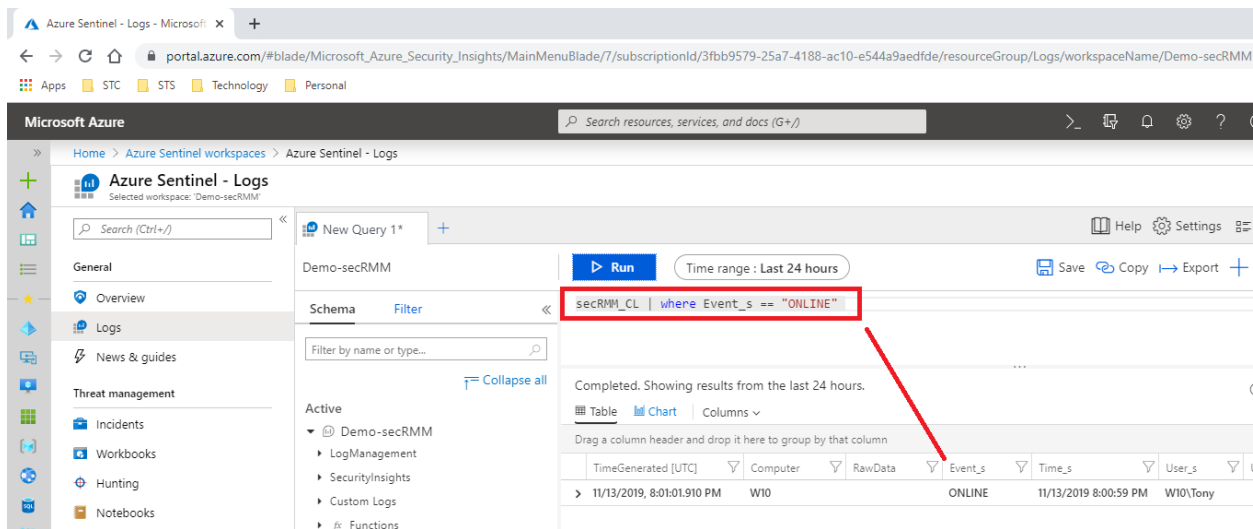
Azure uses a query language named “Keyword Query Language” (KQL). The samples below will show you KQL for the secRMM security events.

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)
```

secRMM Azure Sentinel 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 the 'ERRORS' view for the 'Demo-secRMM' workspace. A KQL query is entered in the query editor:

```
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 editor, the results are shown as a table with one row and one column, labeled 'ERRORS'.

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
```

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 the 'New Query 1*' view for the 'Demo-secRMM' workspace. A KQL query is entered in the query editor:

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

The query is highlighted with a red box. Below the query editor, the results are shown as a table with two columns: 'User_s' and 'count_'. The results are:

User_s	count_
W10/Tony	4

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 to 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 Azure Sentinel 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\Harddisk Volume12
	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 Azure Sentinel 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\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 Azure Sentinel 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\Harddisk Volume9
	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 Event Viewer: localhost, event log secRMM		
Row:	5	Previous Next
	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

secRMM Azure Sentinel Administrator Guide

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"))
```

secRMM Azure Sentinel Administrator Guide

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

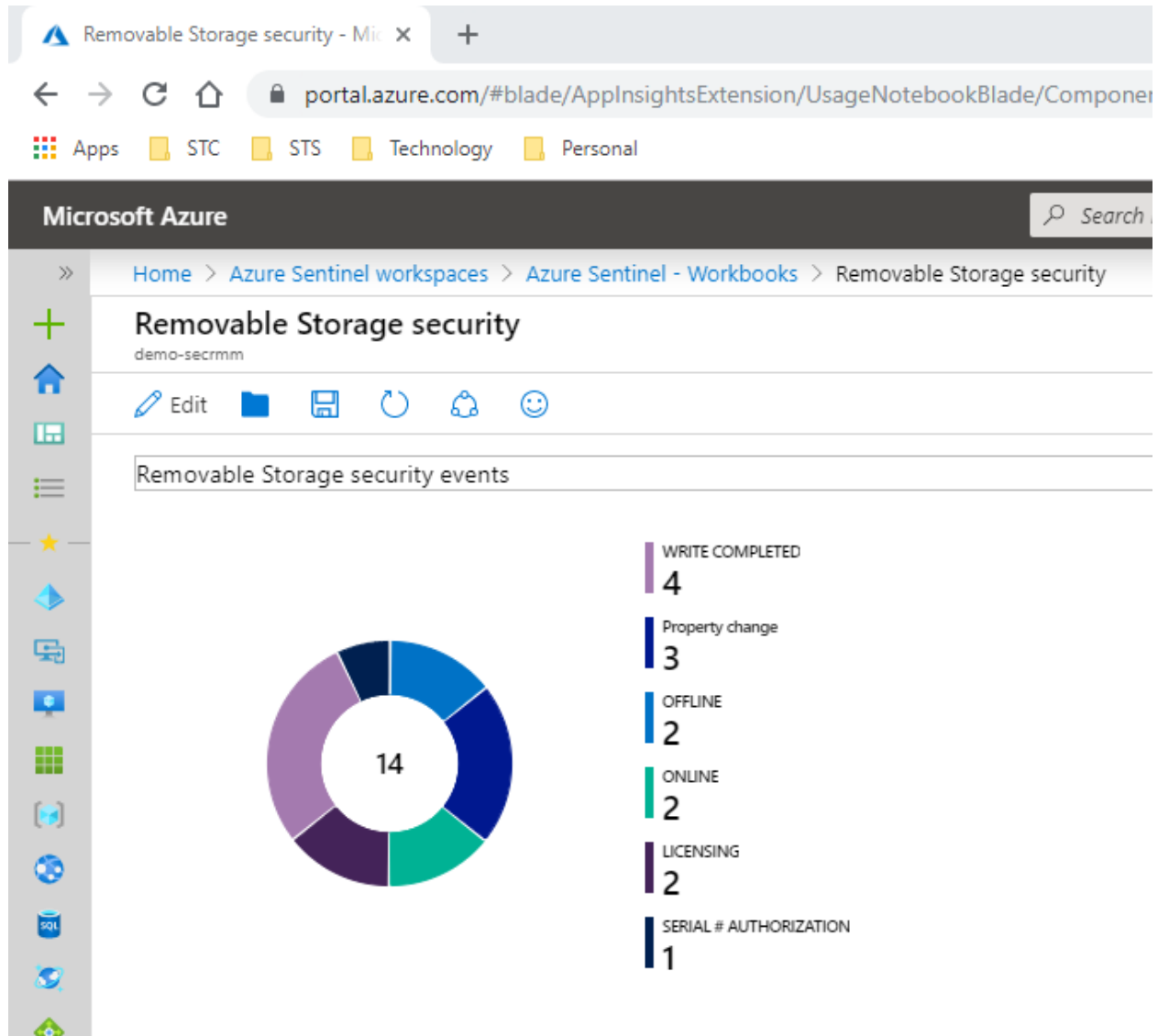
```
secRMM_CL | where ((Event_s == "ONLINE") and (AdditionalProgramInfo_s contains "Mobile device is not MDM enrolled"))
```

secRMM 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 Sentinel Workbook

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

secRMM Azure Sentinel Administrator Guide



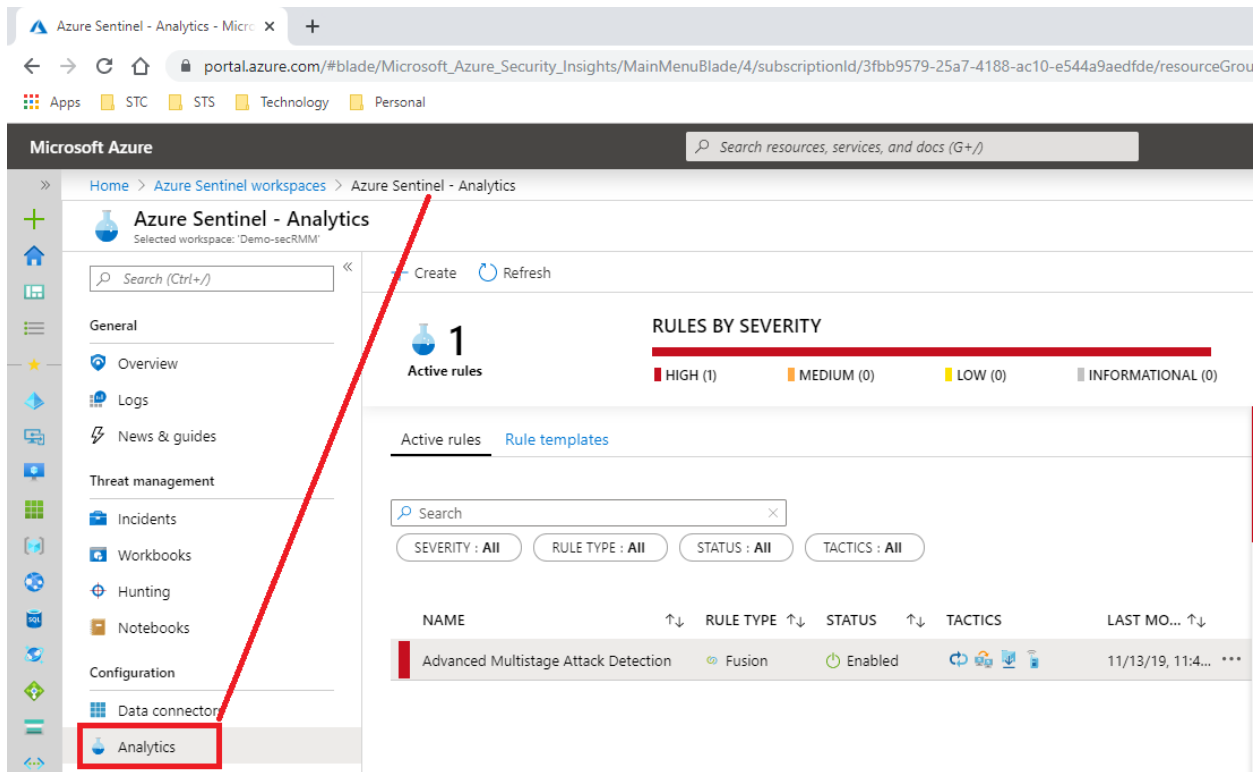
There is currently no method to import a workbook into your Azure Sentinel instance. When a method becomes available from Microsoft, we will update the process for you. For now, please download the json file (which is the Sentinel workbook) on github at: <https://github.com/anthonylamark/secRMMAzureSentinel>

Azure Sentinel Analytics

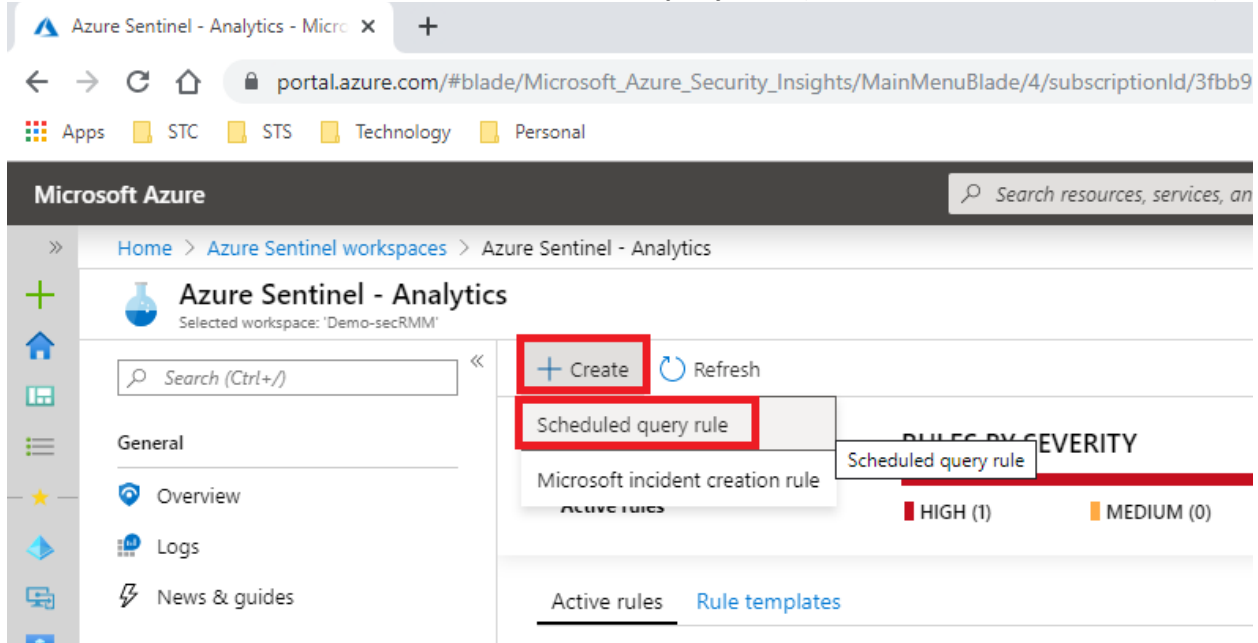
This section will use “Azure Sentinel Analytics” to make your “Azure Sentinel Dashboard” show you when removable storage devices are getting USB mounted (i.e. plugged in, i.e. a secRMM ONLINE event) to the Windows computers in your environment. You may want to integrate other removable storage security 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).

secRMM Azure Sentinel Administrator Guide



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 - Microsoft / x +

portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMe

Apps STC STS Technology Personal

Microsoft Azure

» Home > Azure Sentinel workspaces > Azure Sentinel - Analytics > Rule creation wizard

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 >

secRMM Azure Sentinel Administrator Guide

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
```

Rule creation wizard

[General](#) [Set rule logic](#) [Automated response](#) [Review and create](#)

Define the logic for your new analytic rule.

Rule query

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

Any time details set here will be within the scope defined below in the Query scheduling fields.

[View query results >](#)

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.

Entity Type	Column
Account	Defined in query
Host	Defined in query
IP	<input type="text" value="Choose column"/> ▾

secRMM Azure Sentinel Administrator Guide

Query scheduling

Run query every *

5 ✓

Minutes ✓

Lookup data from the last * ⓘ

5 ✓

Minutes ✓

Stop running query after alert is generated ⓘ

On

Off

Alert threshold

Generate alert when number of query results

Is greater than ✓

*
1 ✓

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

The screenshot shows the Azure Sentinel Rule creation wizard in a web browser. The browser tab is titled 'Rule creation wizard - Microsoft'. The address bar shows the URL: portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4. The breadcrumb navigation is: Home > Azure Sentinel workspaces > Azure Sentinel - Analytics > Rule creation wizard. The page title is 'Rule creation wizard'. A green banner indicates 'Validation passed.' The tabs are: General, Set rule logic, Automated response, and Review and create (highlighted with a red box). The main content area says 'Define the logic for your new analytic rule.' and 'Rule query'. The query is: secRMM_CL | where Event_s == "ONLINE" | extend AccountCustomEntity = User_s | extend HostCustomEntity = Computer. At the bottom, it says 'Any time details set here will be within the scope defined below in the Query scheduling fields.' and 'View query results >'. The left sidebar shows various Azure services icons.

secRMM Azure Sentinel Administrator Guide

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




[Home](#) > [Azure Sentinel workspaces](#) > [Azure Sentinel - Analytics](#) > Rule creation wizard

Rule creation wizard

✓ Validation passed.

[General](#) [Set rule logic](#) [Automated response](#) [Review and create](#)

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

Analytic rule settings

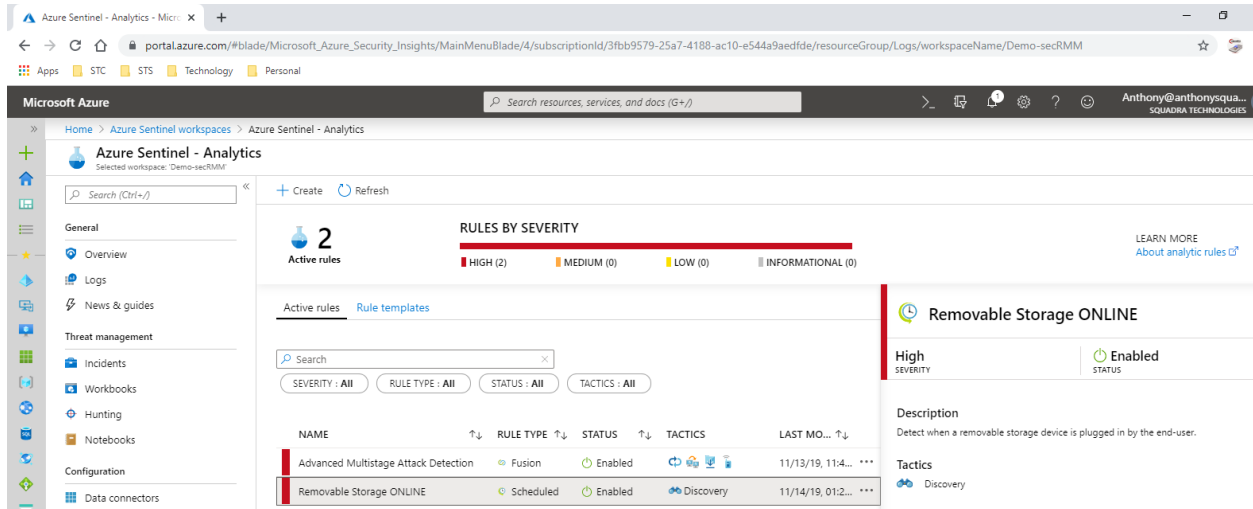
Rule query	secRMM_CL where Event_s == "ONLINE" extend AccountCustomEntity = User_s extend HostCustomEntity = Computer
Rule frequency	Every 5 minutes
Rule period	Last 5 minutes data
Rule threshold	Trigger alert if query returns more than 1 results
Suppression	Not configured

Mapped entities

[Previous](#) [Create](#)

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

secRMM Azure Sentinel Administrator Guide



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 Azure Sentinel 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.

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/