Security Removable Media Manager
(secRMM)

Intune Start Here Guide

Version 9.11.23.0

(November 2023)

Protect your valuable data

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

Disclaimer

Squadra Technologies Administrator Guide
Created - March 2011

Table of Contents

Introduction

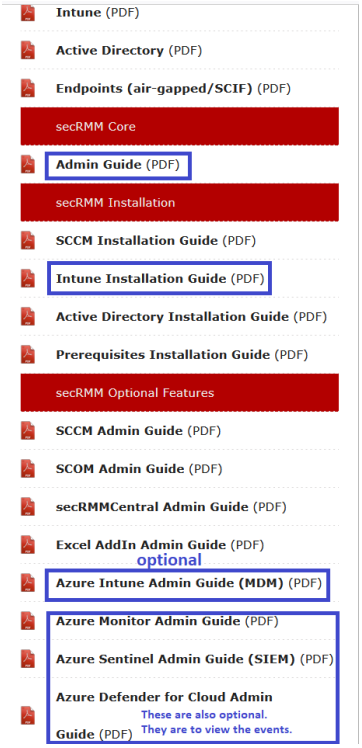
Squadra Technologies *security Removable Media Manager* (**secRMM**) software is Windows security software that runs on your company's workstations and servers. secRMM manages and monitors removable media. In this context, Removable media is defined as external hard disks, USB (flash) drives, smart phones, tablets, SD-Cards, CD-ROM and DVD. 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.

This guide is to help you get started using secRMM in your environment. secRMM can be integrated in many different ways and how you install and use secRMM will depend on how your environment operates. For example, do you use SCCM, Active Directory, Azure or none of these? Regardless of your answer, secRMM can be used in your environment!

Overview

This guide outlines the steps you will perform to use secRMM in your environment:

1. Deploy secRMM to your endpoint computers
2. Centralize the secRMM events generated by your endpoint computers
3. Create secRMM policies for your endpoint computers and/or users
4. View reports and/or dashboard/charts of the secRMM security events



Within an Intune environment, the primary secRMM documents you will use are:

Admin Guide
Intune Installation Guide
Azure Intune Admin Guide (MDM [optional]
Azure Monitor Admin Guide [optional]
Azure Sentinel Admin Guide [optional]
Azure Defender for Cloud Admin Guide [optional]

Step 1: Deploy secRMM to your endpoint computers

The secRMM software needs to "listen" to devices being plugged into the physical USB ports on the computers in your environment. Therefore, secRMM needs to be deployed to each Windows computer (endpoint) in your environment (that you want to be monitored/controlled by secRMM).

Please go to:
https://squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx

In the "secRMM Installation" section, use the "Intune Installation Guide".

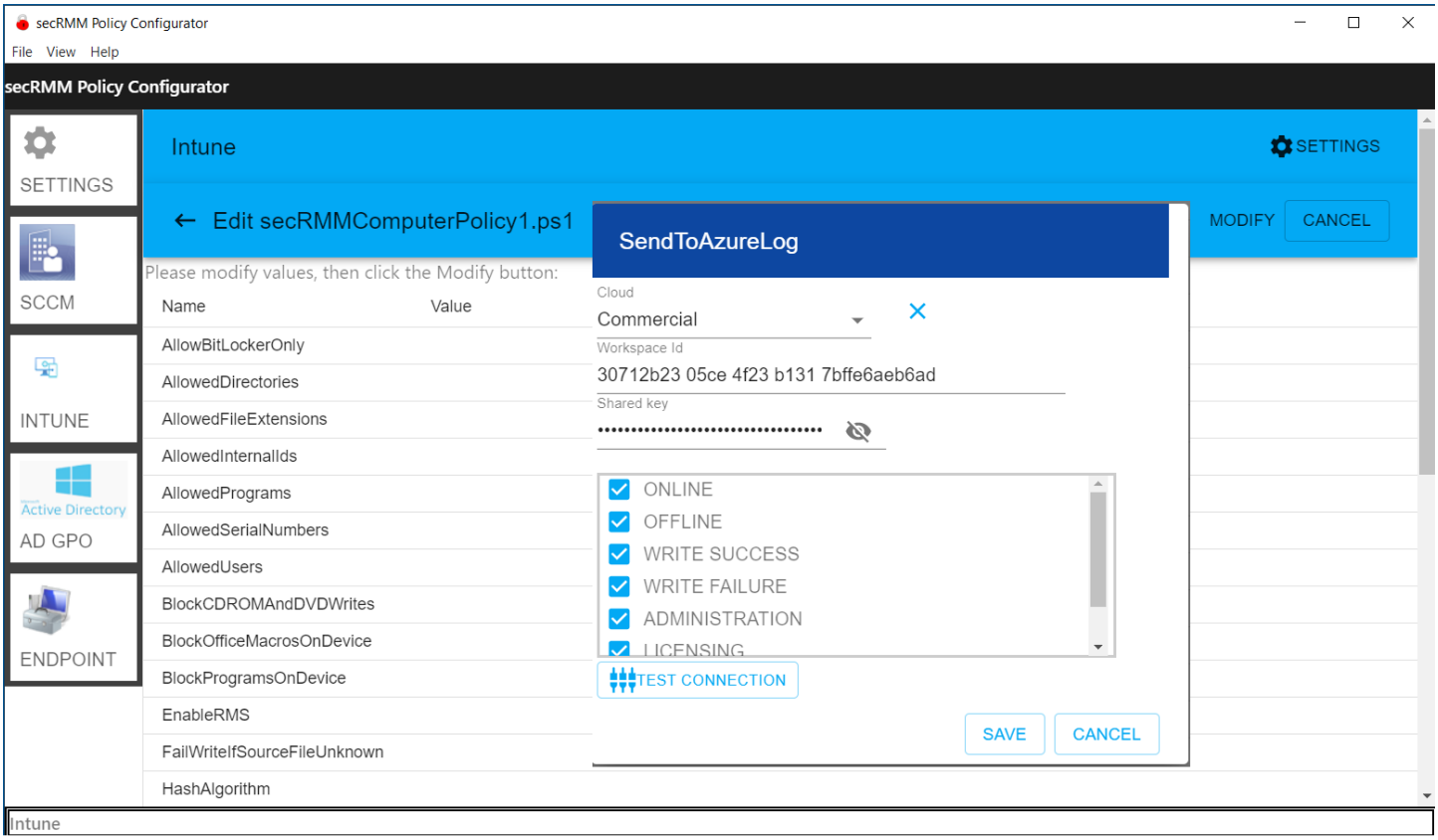
Step 2: Centralize the secRMM events generated by your endpoint computers

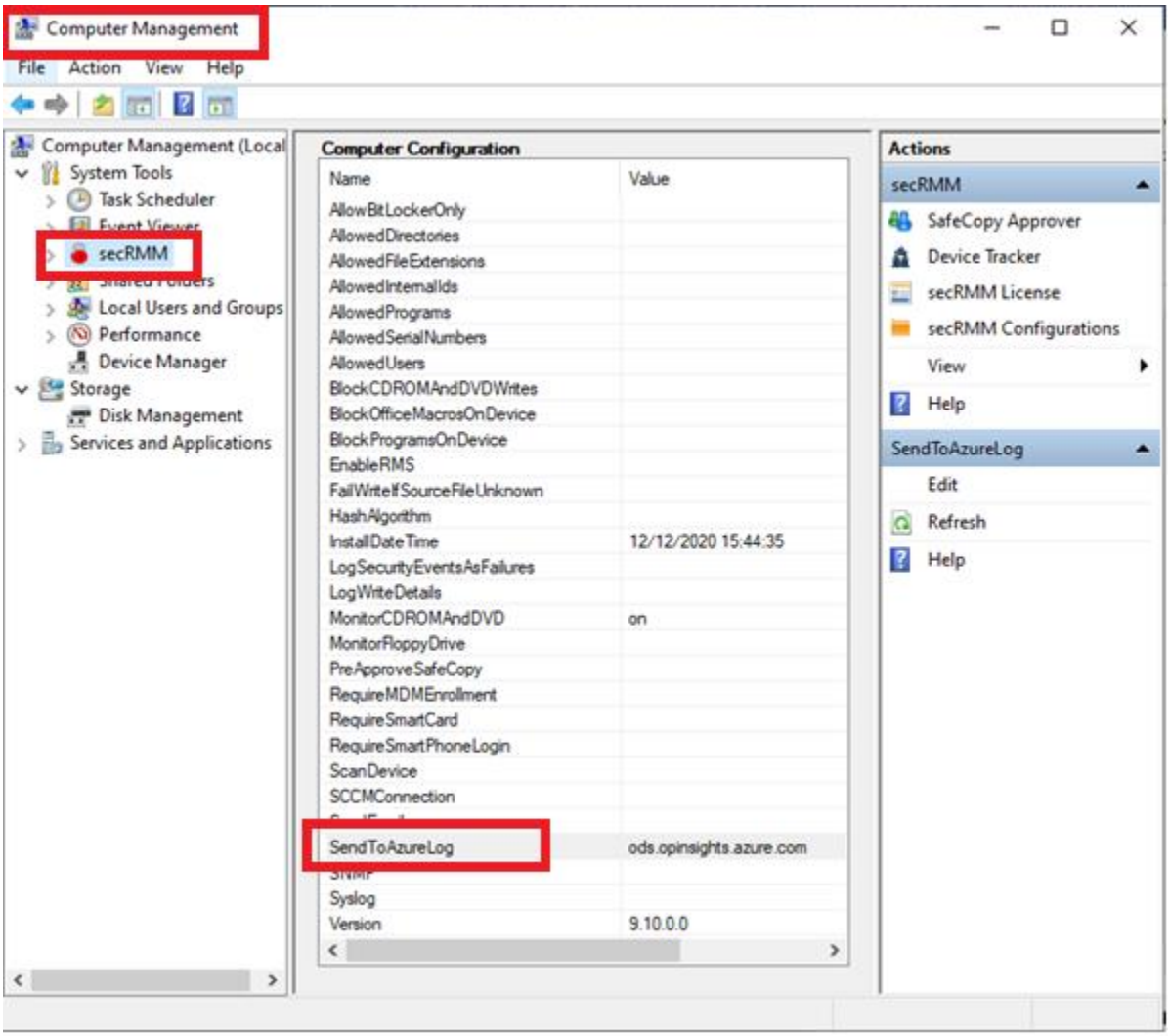
Within your environment, whether you have just 2 computers or 100,000 computers, you will probably want to centralize the events that are being generated by secRMM so you can analyze how users are using removable storage within your environment.

Please go to:
https://squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx

In Azure environments, secRMM stores the secRMM event data in an Azure Log Analytics table. secRMM has a property variable called SendToAzureLog that will need to be setup so that secRMM sends the event data from the endpoint computers to the Azure Log Analytics table. The Azure Monitor, Sentinel and Defender Admin Guides explain how to setup the secRMM **SendToAzureLog** property.

The first screenshot below shows configuring the secRMM SendToAzureLog property using Intune (via the 'secRMM Policy Configurator' tool). Then, the second screenshot show one of the managed Intune Windows endpoint computers with the values you defined in the first screenshot. This is a result of Intune running the PowerShell script on each of the managed windows endpoints (with secRMM installed on it).

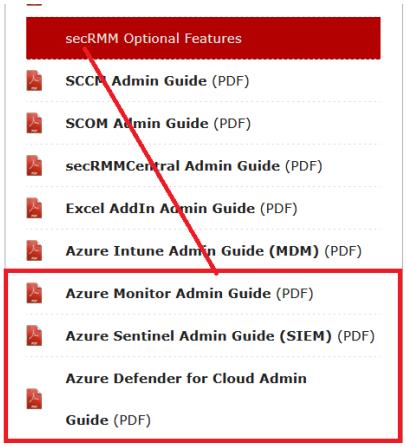

secRMM Policy Configurator
File View Help
secRMM Policy Configurator
SETTINGS
SCCM
INTUNE
Active Directory
AD GPO
ENDPOINT
Intune
SETTINGS
Edit secRMMComputerPolicy1.ps1
MODIFY
CANCEL
Please modify values, then click the Modify button:
Name
Value
AllowBitLockerOnly
AllowedDirectories
AllowedFileExtensions
AllowedInternalIds
AllowedPrograms
AllowedSerialNumbers
AllowedUsers
BlockCDROMAndDVDWrites
BlockOfficeMacrosOnDevice
BlockProgramsOnDevice
EnableRMS
FailWriteIfSourceFileUnknown
HashAlgorithm
SendToAzureLog
Cloud
Commercial
Workspace Id
30712b23 05ce 4f23 b131 7bffe6aeb6ad
Shared key
ONLINE
OFFLINE
WRITE SUCCESS
WRITE FAILURE
ADMINISTRATION
LICENSING
TEST CONNECTION
SAVE
CANCEL
Intune



From the Azure Log Analytics table, you can choose to use one or more of the following Azure services:

Azure Monitor
Azure Sentinel
Azure Defender for Cloud

In the "secRMM Optional Features" section, you might use the one of these documents depending on which Azure services you are using in your environment:
"Azure Monitor Admin Guide"
"Azure Sentinel Admin Guide"
"Azure Defender for Cloud Admin Guide".



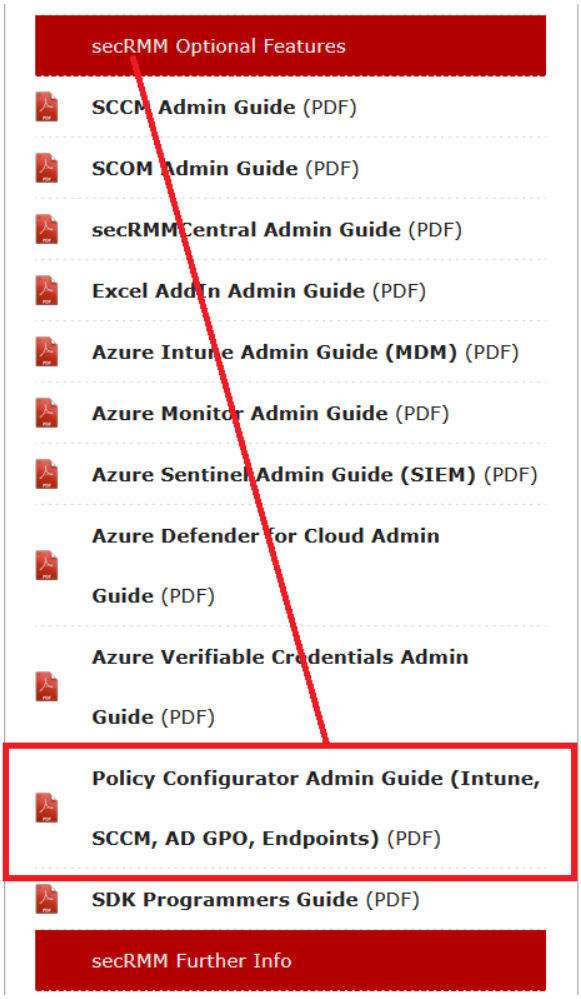
Using an Azure Log Analytics table is just one of many other (or in combination) options you have for sending secRMM security events to different collectors (ex: SCCM/ConfigMgr, email, syslog, Teams, SQL, SNMP).

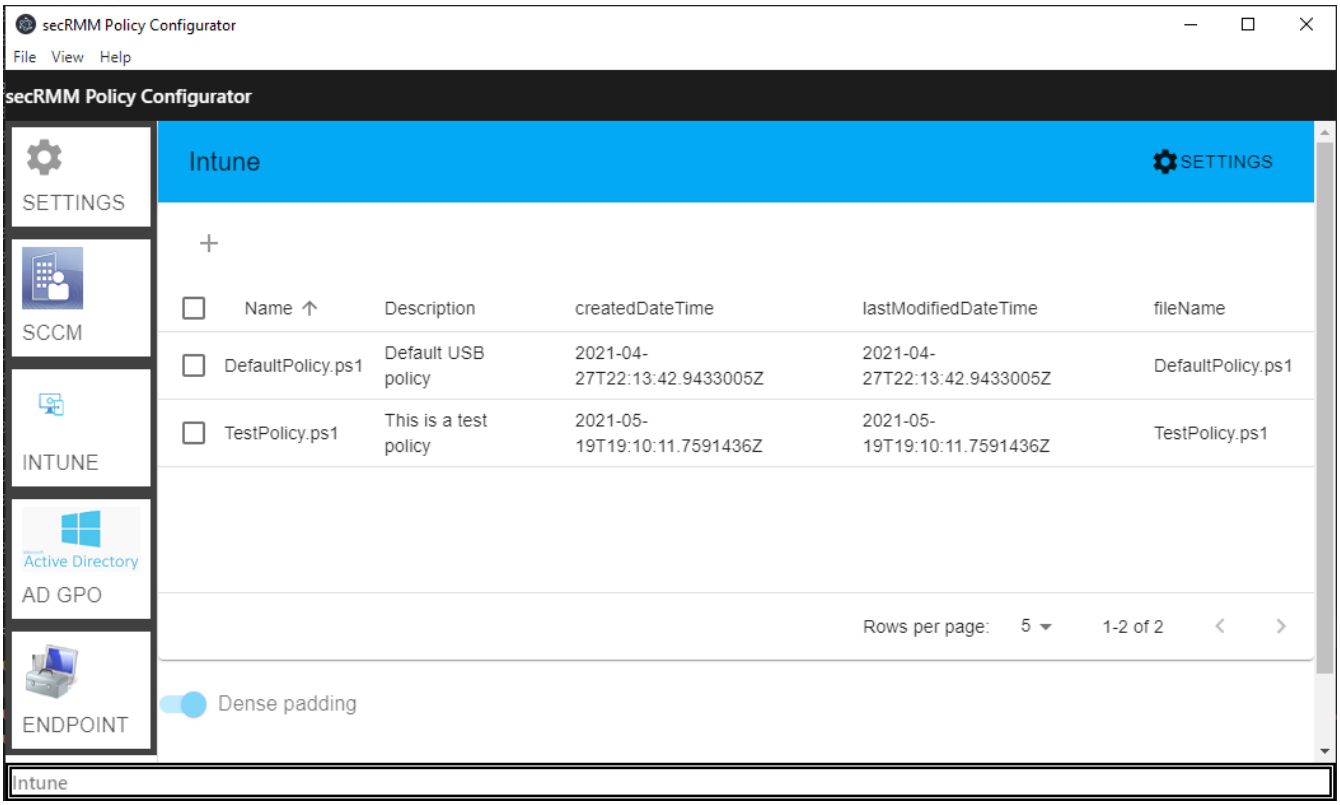
Step 3: Create secRMM policies for your endpoint computers and/or users

In addition to being an auditing tool, secRMM can be configured to control who can use removable storage within your environment and/or only allow certain removable storage devices (or types).

To configure policies within Intune, please use the secRMM Policy Configurator. The secRMM Policy Configurator is an available download on the Squadra Technologies web site.

The documentation for the secRMM Policy Configurator is available in the "secRMM Optional Features" section at:
https://squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx


secRMM Optional Features
SCCM Admin Guide (PDF)
SCOM Admin Guide (PDF)
secRMM Central Admin Guide (PDF)
Excel AddIn Admin Guide (PDF)
Azure Intune Admin Guide (MDM) (PDF)
Azure Monitor Admin Guide (PDF)
Azure Sentinel Admin Guide (SIEM) (PDF)
Azure Defender for Cloud Admin Guide (PDF)
Azure Verifiable Credentials Admin Guide (PDF)
Policy Configurator Admin Guide (Intune, SCCM, AD GPO, Endpoints) (PDF)
SDK Programmers Guide (PDF)
secRMM Further Info

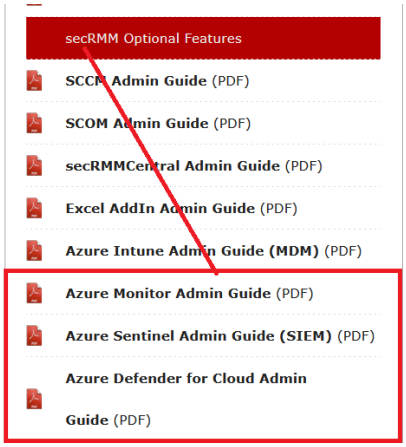


Step 4: View reports and/or dashboard/charts of the secRMM security events

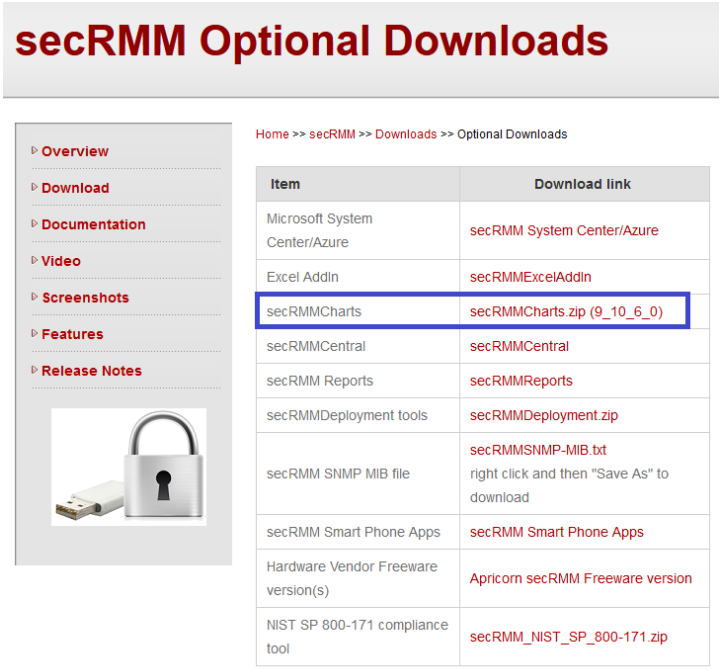
The secRMM software comes with powerful reports (in Azure, they are really Azure workbooks) for analyzing how removable storage is being used in your environment. The secRMM software also comes with a "Live" dashboard/charts that let you see removable storage events in real-time.

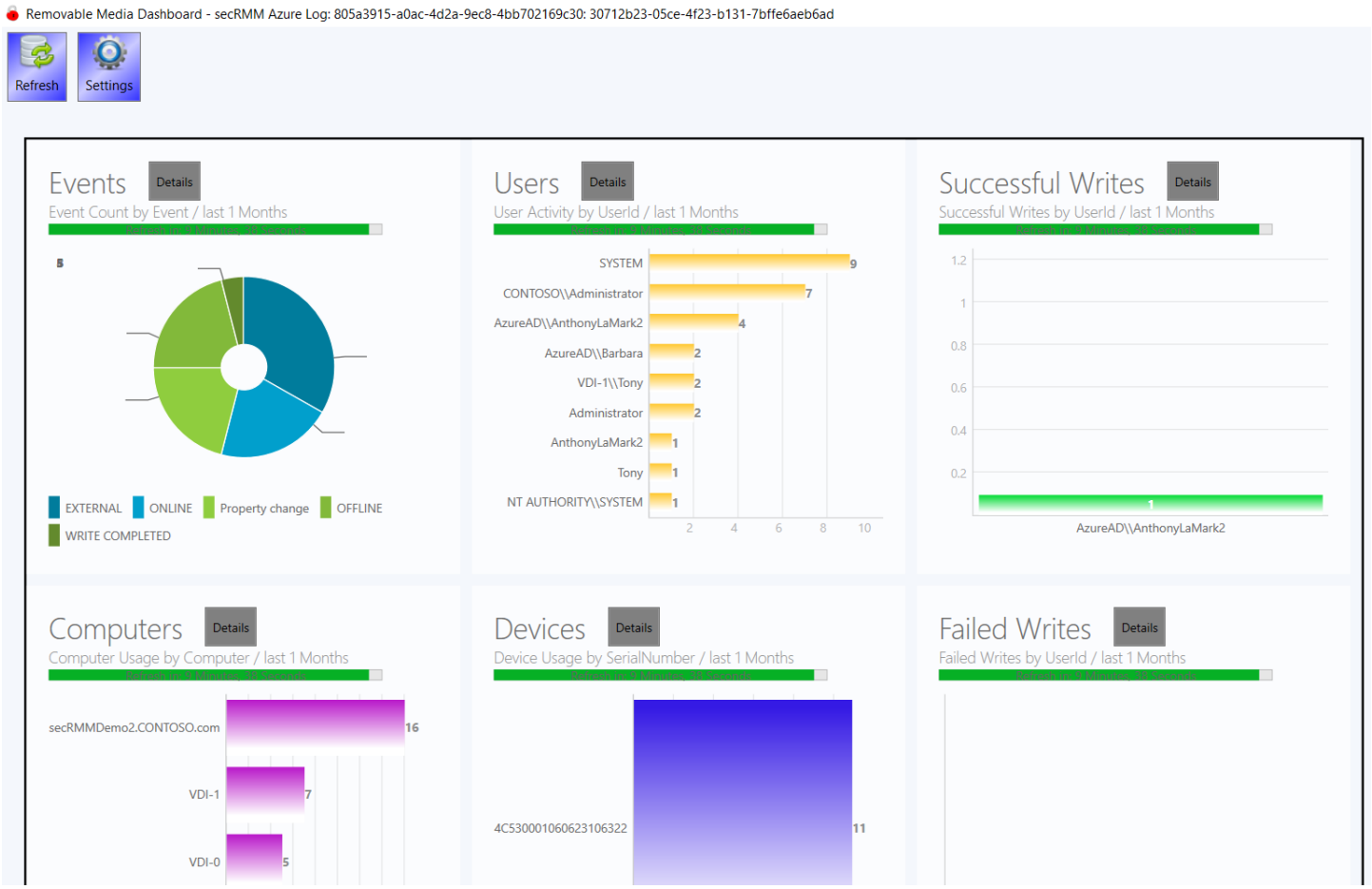
Please go to:
https://squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx

In the "secRMM Optional Features" section, use one or more of:
"Azure Monitor Admin Guide"
"Azure Sentinel Admin Guide"
"Azure Defender for Cloud Admin Guide".



The dashboard/charts are available as a separate download as shown in the screenshot below.





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/