



Security Removable Media Manager
(secRMM)

Intune Start Here Guide

Version 9.11.23.0

(November 2023)

Protect your valuable data



secRMM Intune Start Here 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 Administrator Guide
Created - March 2011

Table of Contents

- INTRODUCTION4
- OVERVIEW.....4
- STEP 1: DEPLOY SECRMM TO YOUR ENDPOINT COMPUTERS5
- STEP 2: CENTRALIZE THE SECRMM EVENTS GENERATED BY YOUR ENDPOINT COMPUTERS5
- STEP 3: CREATE SECRMM POLICIES FOR YOUR ENDPOINT COMPUTERS AND/OR USERS8
- STEP 4: VIEW REPORTS AND/OR DASHBOARD/CHARTS OF THE SECRMM SECURITY EVENTS10
- CONTACTING SQUADRA TECHNOLOGIES SUPPORT12
- ABOUT SQUADRA TECHNOLOGIES, LLC.12

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!

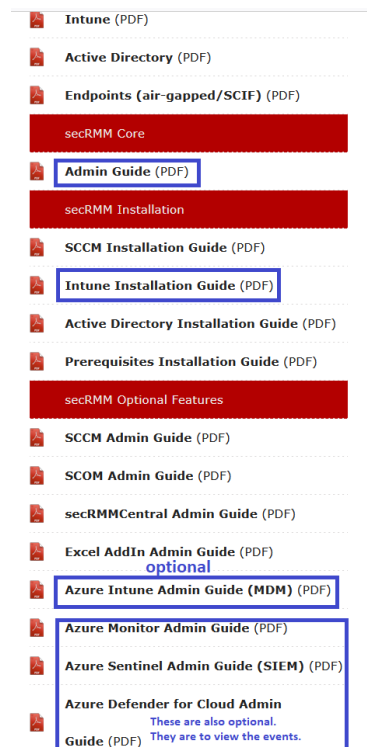
Overview

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]



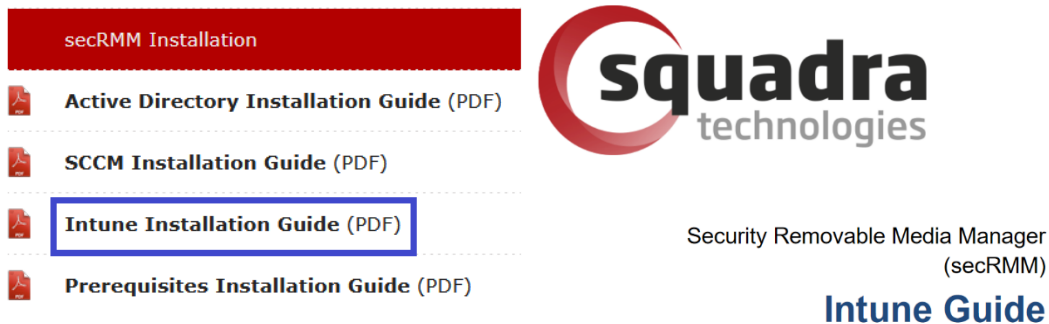
Step 1: Deploy secRMM to your endpoint computers

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”.



secRMM Installation

- Active Directory Installation Guide (PDF)
- SCCM Installation Guide (PDF)
- Intune Installation Guide (PDF)**
- Prerequisites Installation Guide (PDF)

squadra
technologies

Security Removable Media Manager
(secRMM)

Intune 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).

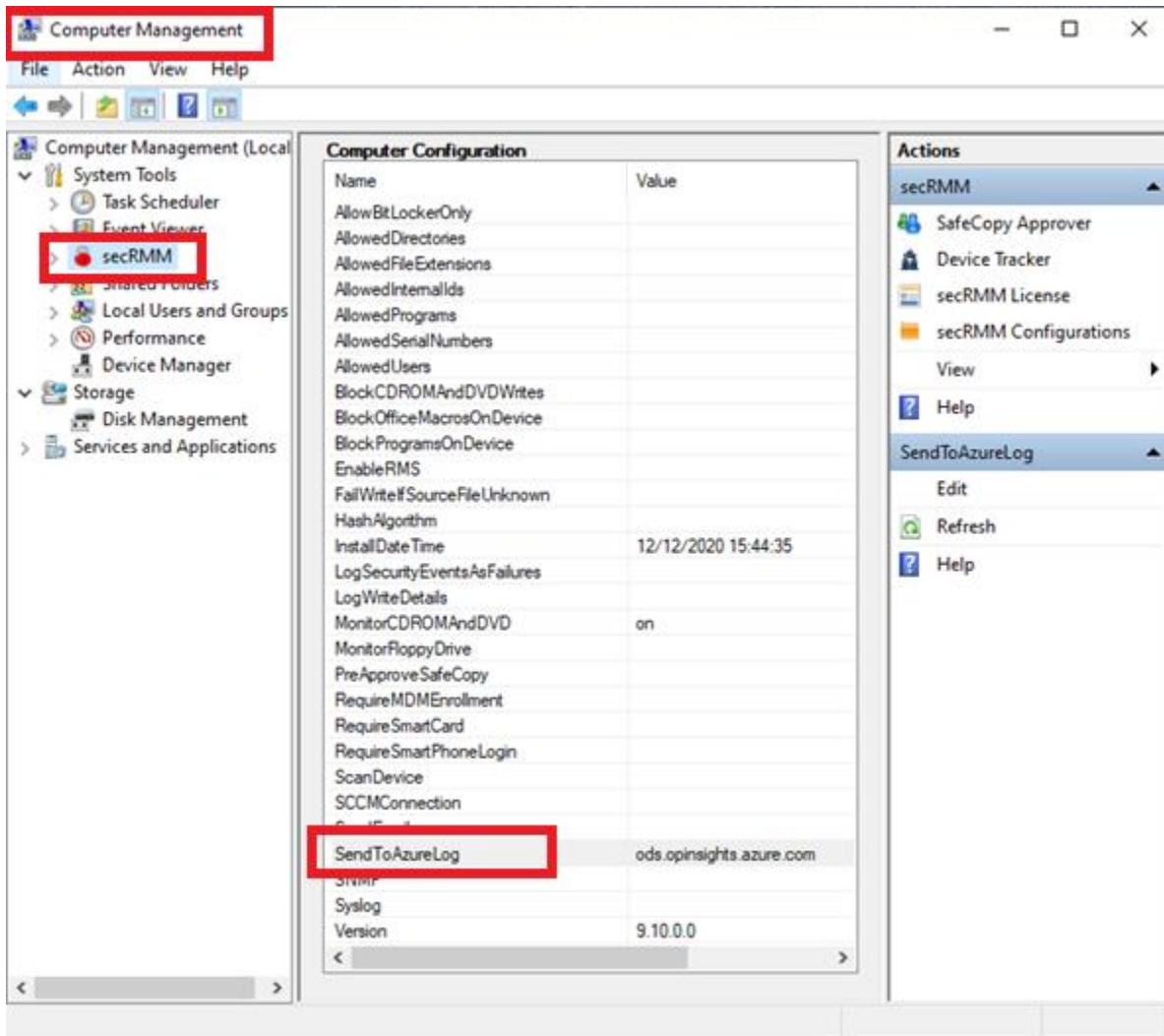
secRMM Intune Start Here Guide

The screenshot displays the 'secRMM Policy Configurator' application window. The main interface is titled 'Intune' and shows a configuration page for 'Edit secRMMComputerPolicy1.ps1'. A modal dialog box titled 'SendToAzureLog' is open, allowing users to modify values for the 'SendToAzureLog' policy. The dialog includes a table for configuration parameters and a list of checked options.

Name	Value
AllowBitLockerOnly	Cloud
AllowedDirectories	Commercial
AllowedFileExtensions	Workspace Id
AllowedInternalIds	30712b23 05ce 4f23 b131 7bffe6aeb6ad
AllowedPrograms	Shared key
AllowedSerialNumbers
AllowedUsers	<input checked="" type="checkbox"/> ONLINE <input checked="" type="checkbox"/> OFFLINE <input checked="" type="checkbox"/> WRITE SUCCESS <input checked="" type="checkbox"/> WRITE FAILURE <input checked="" type="checkbox"/> ADMINISTRATION <input checked="" type="checkbox"/> LICENSING
BlockCDROMAndDVDWrites	<input type="button" value="TEST CONNECTION"/>
BlockOfficeMacrosOnDevice	
BlockProgramsOnDevice	
EnableRMS	
FailWriteIfSourceFileUnknown	
HashAlgorithm	

Buttons: MODIFY, CANCEL, SAVE, CANCEL

secRMM Azure Start Here Guide



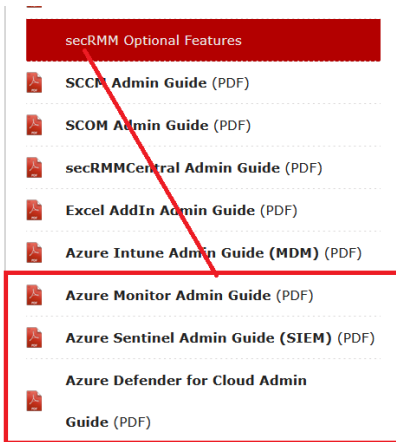
From the Azure Log Analytics table, you can choose to use one or more of the following Azure services:

- 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".

secRMM Intune Start Here 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 Azure Start Here Guide

secRMM Optional Features

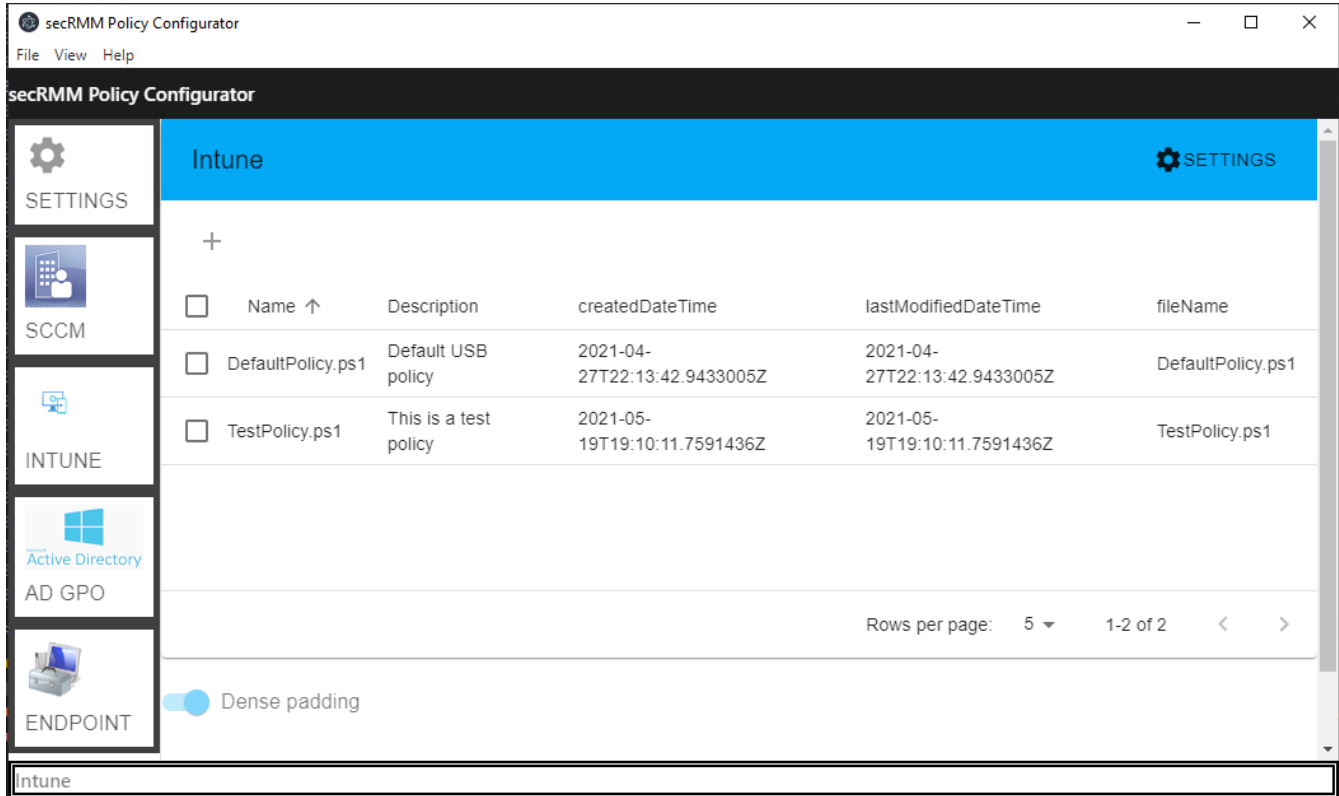
-  **SCCM Admin Guide (PDF)**
-  **SCOM Admin Guide (PDF)**
-  **secRMM Central Admin Guide (PDF)**
-  **Excel Add In Admin Guide (PDF)**
-  **Azure Intune Admin Guide (MDM) (PDF)**
-  **Azure Monitor Admin Guide (PDF)**
-  **Azure Sentinel Admin Guide (SIEM) (PDF)**
-  **Azure Defender for Cloud Admin 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

secRMM Intune Start Here Guide



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>

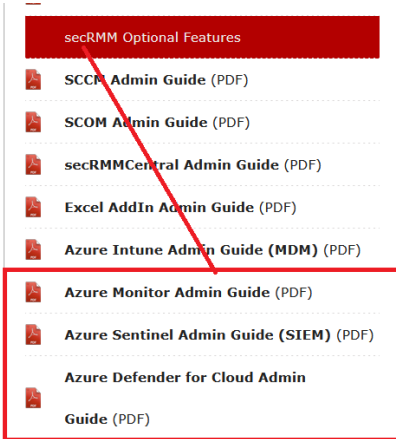
In the “secRMM Optional Features” section, use one or more of:

“Azure Monitor Admin Guide”

“Azure Sentinel Admin Guide”

“Azure Defender for Cloud Admin Guide”.

secRMM Azure Start Here Guide




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

secRMM Optional Downloads

Home >> secRMM >> Downloads >> Optional Downloads

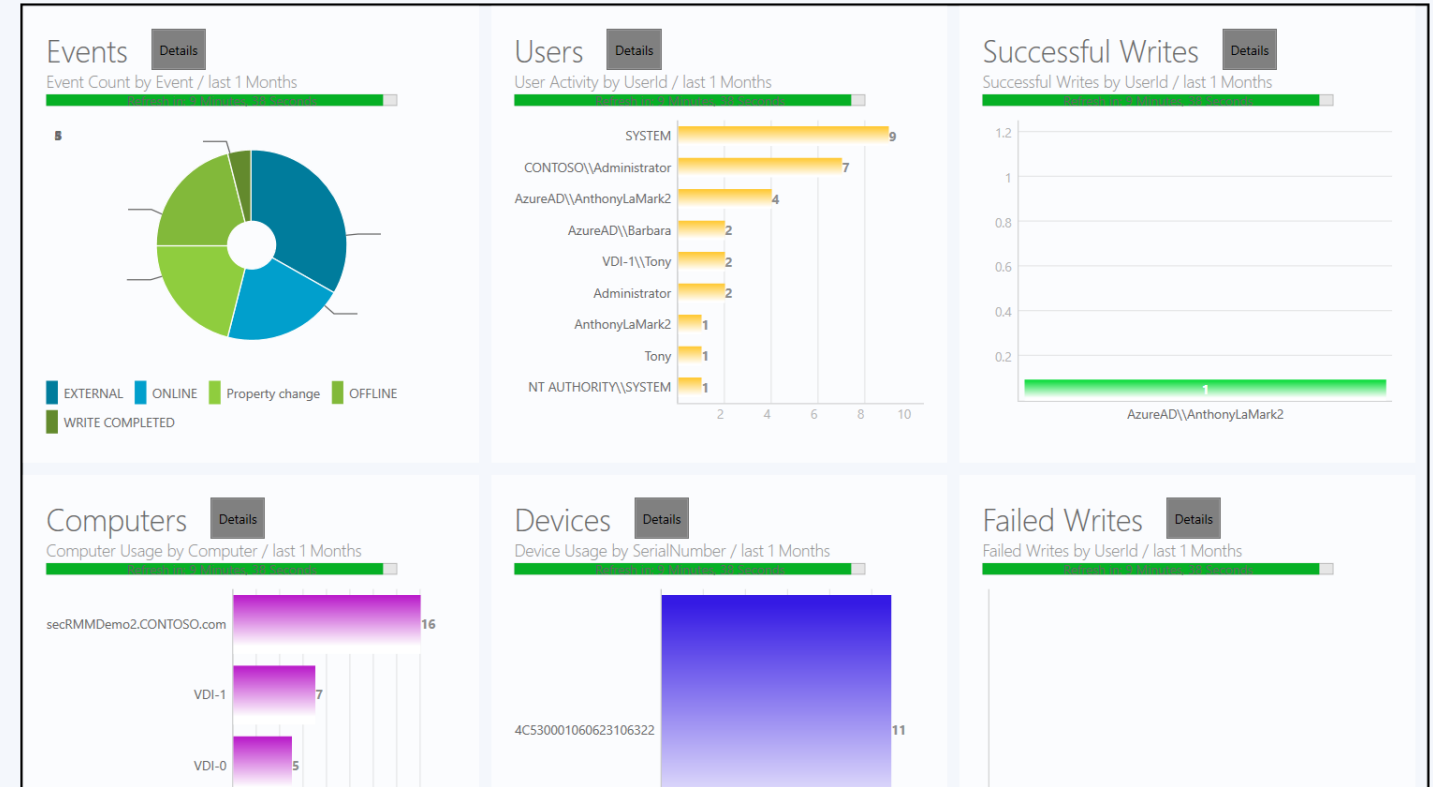
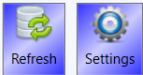
Overview
Download
Documentation
Video
Screenshots
Features
Release Notes



Item	Download link
Microsoft System Center/Azure	secRMM System Center/Azure
Excel AddIn	secRMMExcelAddIn
secRMMCharts	secRMMCharts.zip (9_10_6_0)
secRMMCentral	secRMMCentral
secRMM Reports	secRMMReports
secRMMDeployment tools	secRMMDeployment.zip
secRMM SNMP MIB file	secRMMSNMP-MIB.txt right click and then "Save As" to download
secRMM Smart Phone Apps	secRMM Smart Phone Apps
Hardware Vendor Freeware version(s)	Apicom secRMM Freeware version
NIST SP 800-171 compliance tool	secRMM_NIST_SP_800-171.zip

secRMM Intune Start Here Guide

Removable Media Dashboard - secRMM Azure Log: 805a3915-a0ac-4d2a-9ec8-4bb702169c30: 30712b23-05ce-4f23-b131-7bffe6aeb6ad



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.

secRMM Azure Start Here Guide

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/>