



Security Removable Media Manager
(secRMM)

SCCM Start Here Guide

Version 9.11.27.0

(April 2024)

Protect your valuable data



secRMM SCCM 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 USERS6

STEP 4: VIEW REPORTS AND/OR DASHBOARD/CHARTS OF THE SECRMM SECURITY EVENTS7

CONTACTING SQUADRA TECHNOLOGIES SUPPORT7

ABOUT SQUADRA TECHNOLOGIES, LLC.8

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 a SCCM environment, the primary secRMM documents you will use are:

Admin Guide
SCCM Installation Guide
SCCM Admin Guide

secRMM Documentation



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 “SCCM Installation Guide”.



Security Removable Media Manager

SCCM 2012
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 the “secRMM Optional Features” section, use the “SCCM Admin Guide”.

Follow the steps in the INSTALLATION section.

secRMM SCCM Start Here Guide

secRMM Optional Features

-  **SCCM Admin Guide (PDF)**
-  **SCOM Admin Guide (PDF)**
-  **secRMMCentral Admin Guide (PDF)**
-  **Excel AddIn Admin Guide (PDF)**
-  **Azure Intune Admin Guide (MDM) (PDF)**
-  **Azure Sentinel Admin Guide (SIEM) (PDF)**
-  **SDK Programmers Guide (PDF)**

INSTALLATION	
Downloads used in this document	
SCCM secRMM CONSOLE EXTENSION	
Prerequisites.....	
SCCM Features.....	
Required SCCM permissions	
Install the secRMM SCCM Console Extension	
Start the SCCM Console to verify installation	
Uninstalling the secRMM SCCM Console Extension	
SCCM secRMM STATUS MESSAGES.....	
Step 1 - Setting up the SCCM site server.....	
Step 2 - Setting up the secRMM "SCCMConnection" property	
SCCM Security Role	
SCCM Admins Group	
SCCM Security Scope	
Step 3 - Create a SCCM Status Message query for "removable media" events.....	

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).

Please go to:

<https://squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx>

In the "secRMM Optional Features" section, use the "SCCM Admin Guide".
Follow the steps in the USAGE AND CONFIGURATION section.

secRMM Optional Features

-  **SCCM Admin Guide (PDF)**
-  **SCOM Admin Guide (PDF)**
-  **secRMMCentral Admin Guide (PDF)**
-  **Excel AddIn Admin Guide (PDF)**
-  **Azure Intune Admin Guide (MDM) (PDF)**
-  **Azure Sentinel Admin Guide (SIEM) (PDF)**
-  **SDK Programmers Guide (PDF)**

USAGE AND CONFIGURATION.....	
SCCM secRMM CONSOLE EXTENSION	
Create a Removable Media Policy	
Deploy a Removable Media Policy	
Deploy a Removable Media Policy using SCCM Compliance Settings ...	
Computer versus User deployment	
User deployment requirements	
Windows successful logon event.....	
Computer policy with SCCMConnection property defined	
Microsoft ".NET Framework 3.5"	
Verifying the computer policy deployment.....	
Verifying the user policy deployment.....	
Remediation	
Editing a Removable Media Policy.....	
Deleting a Removable Media Policy.....	
Copying an existing Removable Media Policy.....	

To understand the security policies and controls that secRMM can apply, please go to:
<https://squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx>

and in the "secRMM Core" section, use the "Admin Guide".

secRMM Core



Admin Guide (PDF)

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

The secRMM software comes with powerful reports 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 the “SCCM Admin Guide”.
Follow the steps in the INSTALLATION section.

secRMM Optional Features



SCCM Admin Guide (PDF)



SCOM Admin Guide (PDF)



secRMMCentral Admin Guide (PDF)



Excel AddIn Admin Guide (PDF)



Azure Intune Admin Guide (MDM) (PDF)



Azure Sentinel Admin Guide (SIEM) (PDF)



SDK Programmers Guide (PDF)

SCCM secRMM REPORTS	
Prerequisites.....	
Install the SCCM secRMM reports.....	
Install secRMM reports assembly.....	
Load secRMM reports into SSRS.....	
Load secRMM reports into SSRS using Powershell...	
Load secRMM reports into SSRS manually	

Within SCCM, the dashboard/charts are available right within the SCCM console (see Monitoring->Security within the SCCM console treeview). You can also run the dashboard/charts outside of the SCCM console using the data within the SCCM database.

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/