

Security Removable Media Manager SCOM 2012 Administrator Guide

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

Table of Contents

TABLE OF CONTENTS	3
INTRODUCTION	4
INSTALLATION	4
Install the secRMM SCOM Management Pack	4
INSTALL THE SECRMM SCOM REPORTS	11
Register the secRMM .Net assembly into SQL	11
Load secRMM reports into Microsoft SQL Server Reporting Services (SSRS)	15
Load secRMM reports into SSRS using Powershell	15
Load secRMM reports into SSRS manually	15
SCOM AND MANAGEMENT PACK FEATURES	25
COMPUTER MANAGEMENT MMC	25
SCOM SECRMM TASKS	26
Available Reports	30
CONTACTING SQUADRA TECHNOLOGIES SUPPORT	31
ABOUT SQUADRA TECHNOLOGIES, LLC	31

Introduction

Security Removable Media Manager (secRMM) is Windows security software that secures the use of smartphones, tablets, usb/flash drives and other removable media devices. secRMM integrates into Microsoft System Center Operations Manager (SCOM) by providing a SCOM Management Pack (MP) and SCOM reports. The secRMM reports can exist in either (or both) the SCOM run-time data warehouse database (**DW**) and the SCOM Audit and Collection (**AC**) database.

Please follow the steps in the next section to begin the installation.

Installation

Install the secRMM SCOM Management Pack

 Download the secRMM Management Pack from the Squadra Technologies web site at <u>http://www.squadratechnologies.com/Products/secRMM/SystemCenter/secRMMSystemCenter</u> <u>OperationsManager.aspx</u> to a directory on your local hard drive (for example: C:\temp\secRMM\SCOMSetup). The secRMM Management Pack file name is **Squadra.secRMM.xml**. There is also a secRMMCentral Management Pack named **Squadra.secRMMCentral.xml**. The procedure for using secRMMCentral has the same steps outlined below.

Please note that if you use the secRMMCentral Management Pack, the computer with secRMMCentral running on it **MUST** also have secRMM installed on it as well. Failure to have secRMM installed will result in invalid event data getting inserted into the SCOM database and this will then cause the secRMM SCOM reports to fail to execute.

- 2. Open the SCOM Console using a userid that is a SCOM Administrator.
- 3. Within the SCOM Console, select "Administration" view

Monitoring	
Authoring	
Reporting	
🚳 Administration	
My Workspace	

4. In the Administration view, right mouse click on "Management Packs". From the pop-up menu, select "Import Management Packs..."



5. In the "Import Management Packs" dialog, click the Add drop-down button and then select "Add from disk...".

	Import Ma	nagement Packs	X
Select Manageme	nt Packs		
Select Management Packs			🕡 Help
	Import list :	Version	Add Properties X Remove Add from catalog Rele Add from disk

6. Select "No" when the "Online Catalog Connection" message box appears.

	Online Catalog Connection	x
?	Some of the management packs you select may have dependencies that cannot be located locally. Would you like to search the online catalog for these dependencies?	
	Yes No	

	Select Manager	nent Packs to import	×
€ 🗇 ד 1 🌗	C:\temp\secRMM\SCOMSetup	✓ C Search SC	COMSetup 🔎
Organize 👻 New	folder		i 🕶 🖬 🔞
🚺 Downloads	^ Name ▲	Date modified	Type Size
🕮 Recent places	Squadra.secRMM.xml	6/30/2013 1:17 PM	XML Document
Figure 7 This PC Desktop Documents Downloads Music Pictures Videos Local Disk (C:)	=		
	File name: Squadra.secRMM.xml	All Mana Ope	igement Packs (*.mp; * ¥ m Cancel

7. Select the secRMM Management Pack that you downloaded in step 1

8. Click the "Install" button.

-	Import Manageme	ent Packs				x
Select Managemer	nt Packs					
Select Management Packs						🕢 Help
	Import list :		🕂 Add 🗕	Propert	ies 🗙 Re	move
	Name	Version	Release Date	Status	License Terms	
	Security for Removable Media (se	9.0.0.0				
	Status details :					
	I his management pack is ready to impor					
				Inst	all (Cancel

9. When the import completes, you will see a status of "Imported". Click the "Close" button at the bottom of the "Import Management Packs" dialog.

Import Management Packs								
Import Manageme	ent Packs							
Select Management Packs				🕜 Help				
	Downloading and importing the selected manager	ient packs.						
	Name	Version	Status					
	✓ Security for Removable Media (secRMM) Librar	y 9.0.0.0	Imported					

10. From the Administration view, you will see the secRMM Management Pack in the list of "Management Packs". You may need to hit refresh several times depending on the workload of your SCOM environment.

Management Packs - SCOMR2 - Op							
File Edit View Go Tasks Tools Help							
Search 👻 📮 🌆 Scope 👂	Find 🔁 Tasks 🕡 🝦						
Administration	Management Packs (100)						
Management Packs	Name	Version	Sealed				
Network Management	🚟 Process Monitoring Library	7.1.10226.0	Yes				
Discovery Rules	🚟 Security for Removable Media (secRMM) Library	9.0.0.0					
Wetwork Devices	📷 SNMP Library	7.0.8433.0	Yes				
< III >	📷 Summary Dashboard	7.1.10226.0	Yes				
Discovery Wizard	📷 Synthetic Transactions Library	7.1.10226.0	Yes				
	🚟 System Administration Item Library	7.5.8501.0	Yes				
Monitoring	📷 System Application Log Library	7.0.8433.0	Yes				
Authoring	🚟 System Center Core Library	7.0.8433.0	Yes				
Authoring	🚟 System Center Core Monitoring	7.1.10226.0	Yes				
Reporting	🚟 System Center Core Monitoring Agent Management	7.1.10226.0	Yes				
Administration	🚟 System Center Core Monitoring Reports	7.1.10226.0	Yes				
	🚟 System Center Core Monitoring Views	7.1.10226.0	Yes				
My Workspace	🚟 System Center Data Warehouse Olap Base Library	7.5.3070.0	Yes				
	🚟 System Center Internal Library	7.0.8433.0	Yes				

11. Select the "Monitoring" view



12. In the Monitoring view, in the tree view section, you will see the "Removable Media Alerts" view



13. You can verify which computers (that have the SCOM agent on them) have the secRMM Management Pack associated to them by viewing the Monitoring->"Discovered Inventory" and setting the "Target type" to secRMM. SCOM discoveries (unfortunately) can take up to 48 hours to run so if you do not see the expected results immediately, you need to give the SCOM framework time to process the new secRMM Management Pack you loaded from above. If, after ample time, you do not see any computers associated with the secRMM Management Pack, please contact Squadra Technologies support for assistance in troubleshooting.

Discovered Inventory (secRMM) - SCOMR2 - (Оре	rations Manager						- 0
File Edit View Go Tasks Tools Help		-						
Search 🛪 📮 🛛 🌆 Scope	F	ind 🗵 Tasks 🔞	1	;				
Monitoring	<	Discovered Invent	ory	(secRMM) (1)			> 1	Fasks
4 🧱 Monitoring	^	🔍 Look for:				Find Now	2	0
Active Alerts		State	*	Name	Path		Stat	e Actions
	-	🕢 Healthy		Squadra.secRMM.Event	SCOMR2.CO	ONTOSO.com		Change Target Type
Maintenance Schedules							1	Start Maintenance Mode
🛃 Task Status							12	Edit Maintenance Mode Settings
UNIX/Linux Computers							100	Ston Maintenance Mode
Windows Computers							-	stop maintenance mode
Agentless Exception Monitoring								
Application Monitoring								
N 🧮 Data Warabaura	Ť							
Channes III de Manue								
Show or Hide Views								
New View 🕨								
Monitoring								
Authoring								
Reporting								

14. Once the SCOM discovery occurs, all Windows computers being monitored by SCOM that have secRMM installed will forward the secRMM alerts (from the secRMM Windows Event Log) into the SCOM console.

	Removable Media Alerts - SCOMR2 - Operations Mar	nager	_ D X
File Edit View Go Tasks Tools Help Image: Search Tasks Image: Search Tasks	🗱 Scope 🔎 Find 🚺 Tasks 🔞 🖕		
Monitoring <	Removable Media Alerts (3)		Tasks
System Center Advisor	Cook for:	d Now Clear	
UNIX/Linux Computers	Severity 🚯 Icon Path Nam	e	Alert Actions
Web Application Transaction Monitoring	Warning A WORKSTATIONA.CONTOSO.com Prop	erty Changed - secRMM	
Process State	Warning 🛕 WORKSTATIONA.CONTOSO.com Prop	erty Changed - secRMM	Subscription
Removable Media Alerts	Warning A WORKSTATIONA.CONTOSO.com Prop	erty Changed - secRMM	Tasks 🗸
iii Windows Service State	<	>	Navigation 🗸
< III >	Alert Details	~	secRMM Tasks
Show or Hide Views New View ▶	Property Changed - secRMM	Alert Des	Authorize Internal Ids
Monitoring	Source: 🛃 Squadra.secRMM.Event Full Path Name: WORKSTATIONA.CONTOSO.com\Squadra.sec	Event De CRMM.Event Administ	Authorize Serial Numbers
Authoring	Alert Rule: O secRMM Property Changed	Action: si Property	Authorize Users
- Reporting	Created: 12/28/2013 12:13:02 PM	Property	secRMM Lockdown mode
· · · · · · · · · · · · · · · · · · ·		Property	secRMM Monitoring mode
Administration		Status: C	secRMM SafeCopy Approver

Install the secRMM SCOM Reports

There are 2 steps to installing the secRMM SCOM Reports. The first step registers a secRMM .Net assembly into the SQL SCOM database. This assembly parses the secRMM data in the database so the reports can be properly formatted. The second step loads the pre-defined secRMM reports into Microsoft SQL Server Reporting Services (**SSRS**) which is the Microsoft product that is used by SCOM for reports.

The required files for both steps are contained in the zip file named **secRMMOpsMgrDWReports.zip** or **secRMMOpsMgrACSReports.zip** which you download from the Squadra Technologies web site at <u>http://www.squadratechnologies.com/Products/secRMM/secRMMReports.aspx</u>. The first zip file is for the SCOM run-time data warehouse database (**DW**) and the second zip file is for the SCOM Audit and Collection (**AC**) database. The SCOM Audit and Collection database is an optional SCOM feature so it may not be installed in your environment. Unzip the file to a network share (or locally) that you can reach from the Windows computer(s) where the SCOM run-time data warehouse database, the SCOM Audit and Collection (**AC**) database and the Microsoft SQL Reporting Services database resides. These databases may or may not reside on the same Windows computer in your environment.

The unzipped folder will have three subfolders in it: Assembly, Reports and SQLTests.



Register the secRMM .Net assembly into SQL

The process of registering the secRMM .Net assembly is the same whether you are performing the step for the SCOM DW or the SCOM AC data base.

1. On the Windows computer where the data base (either DW or AC) is running, open a CMD window using "Run as Administrator"



2. Go to the directory where you extracted the **secRMMOpsMgrDWReports.zip** or **secRMMOpsMgrACSReports.zip** file. Go into the Assembly subfolder.

- 3. For the following steps below, make sure that the userid you are logged in as has DBO/sysadmin permissions on the database so that the script executes with the proper permissions.
- 4. For the following steps below, check to make sure that all of the files that were unzipped are unblocked (see screen shot below). Windows (sometimes) blocks these files because they were downloaded from the Internet.

secRMMSCC	M2012ConsoleExtension.dll Properties
General Secu	inty Details Previous Versions
2	secRMMSCCM2012ConsoleExtension.dll
Type of file:	Application extension (.dll)
Opens with:	Unknown application Change
Location:	D:\Hold\Downloads\5.5.0.0\secRMMSCCMInstall
Size:	273 KB (280,064 bytes)
Size on disk:	276 KB (282,624 bytes)
Created:	Yesterday, September 08, 2013, 11:55:44 AM
Modified:	Today, September 09, 2013, 6:14:38 PM
Accessed:	Yesterday, September 08, 2013, 11:55:44 AM
Attributes:	Read-only Hidden Advanced
Security:	This file came from another computer and might be blocked to help protect this computer.
	OK Cancel Apply

- 5. Run the script named InstallAssemblyForSCOMDW.cmd (or InstallAssemblyForSCOMAC.cmd) A log file will be generated (it will be the only file with an extension of rpt).
- 6. Review the log file generated. It should not contain any errors. If there are errors, please make sure your userid has DBO/sysadmin permissions to the database.

his PC > Local Disk (C:) > secRMM > secRMMOpsMgrDWReports > Assembly > C Search Assembly P								
Name	Date modified	Туре		Size				
InstallAssemblyForSCOMDW	8/7/2015 2:41 PM	Windows C	Comma	1 KB				
InstallSCOMDW_Output.rpt	12/28/2015 9:07 AM	RPT File		1 KB				
InstallSqlScript.sql	8/7/2015 10:19 AM	SQL File		3 KB				
SCOM_DW_README	12/17/2015 4:22 PM	Text Docur	ment	1 KB				
secRMMSQLScalarValuedFunction.dll	10/8/2015 11:28 AM	Application	n extens	6 KB				
secRMMSQLTableValuedFunction.dll	12/28/2015 8:58 AM	Application	n extens	34 KB				
C:\secRMM\secRMMOpsMgrDWReports\Assembly>type InstallSCOMDW_Output.rpt Changed database context to 'OperationsManagerDW'. AssemblyFile1=C:\secRMM\secRMMOpsMgrDWReports\Assembly\secRMMSQLTableValuedFunct ion.dll CREATE ASSEMBLY1 SUCCEEDED. AssemblyFile2=C:\secRMM\secRMMOpsMgrDWReports\Assembly\secRMMSQLScalarValuedFunc tion.dll CREATE ASSEMBLY2 SUCCEEDED. Configuration option 'clr enabled' changed from 1 to 1. Run the RECONFIGURE stat ement to install. C:\secRMM\secRMMOpsMgrDWReports\Assembly>_								

Load secRMM reports into Microsoft SQL Server Reporting Services (SSRS)

Load secRMM reports into SSRS using Powershell

The Powershell script used in this section performs the steps in the "Load secRMM reports into SSRS manually" subsection below.

- 1. In the command window, change directory (CD) into the temporary directory where you unzipped secRMMSCCMReports.zip.
- 2. Now change directory (CD) into the Reports sub-directory.
- 3. In the Reports sub-directory, you will see a file named ImportReports.cmd and ImportReports.ps1 (as shown in the screenshot below).

This PC > Local Disk (C:) > temp > secRMMOpsMgrDWReports > Reports > SCOM_DW_DB

Name	Date modified	Туре
S ImportReports.cmd	3/1/2019 12:48 PM	Windows Command Script
ImportReports.ps1	3/6/2019 12:36 PM	Windows PowerShell Script
Removable Media Administration Events.rdl	3/6/2019 11:18 AM	RDL File
Removable Media All Events.rdl	3/6/2019 11:29 AM	RDL File
Removable Media Authorization Failure Events.rdl	3/6/2019 11:29 AM	RDL File
Removable Media Charts.rdl	3/6/2019 11:34 AM	RDL File
Removable Media Online-Offline Events.rdl	3/6/2019 11:38 AM	RDL File
Removable Media Write Events.rdl	3/6/2019 11:42 AM	RDL File

4. In the command window, type ImportReports.cmd and hit the enter key. The output will look similar to the screenshot below.

Administrator: Command Prompt
Folder "Removable Media Security" Created
Report Removable Media Administration Events.rdl uploaded successfully.
Report Removable Media All Events.rdl uploaded successfully.
Report Removable Media Authorization Failure Events.rdl uploaded successfully.
Report Removable Media Charts.rdl uploaded successfully.
Report Removable Media Online-Offline Events.rdl uploaded successfully.
Report Removable Media Write Events.rdl uploaded successfully.
Import of reports completed.
C:\temp\secRMMOpsMgrDWReports\Reports\SCOM_DW_DB>_

If the Powershell output looks like the above screenshot, you may skip over the "Load secRMM reports into SSRS manually" subsection below.

Load secRMM reports into SSRS manually

1. On the Windows computer where SSRS is running, open a web browser and go to the URL http://localhost/reports.

5	scomr2 - Remote Desktop Connection	_ _ X
C Reports Pages/Folder.aspx	、 ア・C 🏉 Home - Report Manager	×
SQL Server Reporting Services Home		
📸 New Folder 👘 💆 New Data Source 👘 🕌 Re	eport Builder 🕴 🕍 Folder Settings 🕴 🥀 Upload Fi	le
Application Monitoring	Microsoft.SystemCenter.ClientMonitoring	Microsoft.SystemCenter.DataWarehouse
Microsoft.SystemCenter.DataWarehouse	Microsoft.SystemCenter.OperationsMan	Microsoft.SystemCenter.WebApplication
	System.NetworkManagement.Reports	Users Folders
banner_portrait.jpg	console_tasks_icon.png	console_views_icon.png
gradient_portrait.gif	reports_icon.png	

2. Select the "New Folder" option and create a folder named "Removable Media Security"

5	scomr2 - Remote Desktop Connection
	http://localhost/Reports/Pages/FolderProperties.aspy?Crea.Q.z.C.
Home	Reports/ reports/ reges/ rolder roperties.aspx: Crea 🔎 * O
	Server Reporting Services N Folder
Create a nev	v folder in Home.
Name:	Removable Media Security
Description:	Reports for Removable Media provided by the product secRMM
	Hide in tile view
ОК	Cancel

3. You will see the new folder on the main page. Double click the new folder to go into it.



4. Select the "Upload File" option

scomr2 - Remote Desktop C	scomr2 - Remote Desktop Connection				
← → Ø http://localhost/Reports/Pages/Folder.aspx?ltemPath=%2f タ - c Ø @ Removable	Media Security 🗙				
Home					
SQL Server Reporting Services Removable Media Security					
🞬 New Folder 🔰 🧕 New Data Source 🛛 📓 Report Builder 👘 🕍 Folder Settings	🎕 Upload File				
There are no items in Removable Media Security. Click Help for more information about this pa	ige.				

5. From the "Choose File to Upload", go to the SCOM_DW_DB or SCOM_AC_DB folder (under the directory where you extracted the secRMMOpsMgrDWReports.zip or secRMMOpsMgrACSReports.zip file) depending on which SCOM database you are importing the reports for. Unfortunately, the "Choose File to Upload" dialog only allows you to choose one file

at a time so you must repeat this step 5 times (once for each report).

e		Choose File to Upload	X
€ ⊚ - ↑ 💵	:\Repor	ts\SCOM_DW_DB V C Search S	com_dw_db 🎾
Organize 🔻 New fol	der		III 🔻 🔟 🔞
 Recent places This PC Desktop Documents Downloads Music Pictures Videos Local Disk (C:) secRMMOpsMgr 		Name secRMM_AdministrationEvents_OperationsManagerDW.rdl secRMM_AllEvents_OperationsManagerDW.rdl secRMM_AuthorizationFailureEvents_OperationsManagerDW.rdl secRMM_OnlineOfflineEvents_OperationsManagerDW.rdl secRMM_WriteEvents_OperationsManagerDW.rdl	Date modified 12/27/2013 3:31 PM 12/27/2013 3:31 PM
👊 Network	~ <	III	>
Fil	le name	secRMM_AdministrationEvents_OperationsManager v All Files	: (*.*) ♥ pen Cancel

5	scomr2 - Remote Desktop Connection
Home > Remo	http://localhost/Reports/Pages/Import.aspx?ItemPath= %21 🔎 🗸 🖒 🌠 Upload File - Report Manager ×
	Server Reporting Services Ioad File
Upload a re File to uploa	port (.rdl), model (.smdl), shared dataset (.rsd), report part (.rsc), or other resource into Removable Media Security. ad: X:\Reports\SCOM_DW_DB\secR Browse
Name:	SecRMM_AllEvents_OperationsManagerDvv Overwrite item if it exists Cancel

- 6. When you are finished with the uploads, you will have all the secRMM reports loaded. The last step is to associate the SCOM SQL datasource to each report. Unfortunately, you must repeat the following steps for each report since there is no way to apply it to all the reports at one time.
- 7. To the right of the report name, click the yellow down arrow and select "Manage" from the list.

€€	ا الله http://localhost/Reports/Pa	- d	🦉 Data Warehouse - Report M.	×
Home > S	system Center Operations Manager	> R0	emovable Media Reports	
	Data Warehouse			
🗙 Dele	te 🛛 💣 Move 🕴 🚰 New Folde	er	일 New Data Source 🔰 🗳	Repc
🗌 Туре	Name 🗸			Des
	secRMM_AdministrationEvents_C	pera	ationsManagerDW 🔽	
	secRMM_AllEvents_OperationsM		Move	
	secRMM_AuthorizationFailureEve	X	Delete	
	secRMM_OnlineOfflineEvents_Op	R	Subscribe	
	secRMM_WriteEvents_Operations	E.	Create Linked Report	
			View Benett History	
		8	Security	
		L	Manage	
		¢	Download	
		4	Edit in Report Builder	
	I			

8. In the "Manage" page, click the "Data Sources" tab.

← <> <a> fill http://localhost	/Reports/Pag 🔎 🗸 🖒 🧟 secRMM_AdministrationEv 🗙 🧟 squadra technologies secRMM
Home > System Center Oper	ations Manager > Removable Media Reports > Data Warehouse Home My Subscriptions Si
	rting Services AdministrationEvents_OperationsManagerDW Search
Properties	Data Source1
Parameters	A shared data source A shared data A shared
Data Sources	Select a shared data source Browse 🔥 The shared data source reference is no longer valid
Subscriptions	○ A custom data source
Processing Options	Data source type: Microsoft SQL Server
	Connection string:

9. In the "Manage"->"Data Sources" page, click the "Browse" button in the "A Shared data source" section.

Location: /Data Warehouse Main
🖃 🛅 Home
🚊 🛅 Application Monitoring
🚊 🛅 Microsoft.SystemCenter.ClientMo
🗄 🛅 Microsoft.SystemCenter.DataWar
🚊 🛅 Microsoft.SystemCenter.DataWar
🗒 🛅 Microsoft.SystemCenter.DataWar
🚊 🛅 Microsoft.SystemCenter.Operatio
🗒 🛅 Microsoft.SystemCenter.WebAppl
🗄 🧰 My Reports
🗄 🚞 System Center Operations Manag
🗄 🛅 System.NetworkManagement.Rep
🗄 🛅 Users Folders
🛄 Data Warehouse Main
OK Cancel

Browse folders to select a shared data source to use with this item.

- 10. Click the "Data Warehouse Main" or "Audit and Collection Services" data source (it should be at the very bottom of the list) and then click OK.
- 11. You will now be back on the "Manage"->"Data Sources" page. Make sure you click the "Apply" button on the bottom of the page.

Properties	Data Source1				
Parameters	A shared data source				
Data Sources	/Data Warehouse Main Browse				
Subscriptions	○ A custom data source				
Processing Options	Data source type: Microsoft SQL Server				
Cache Refresh Options	Connection string:				
Report History					
Snapshot Options	Connect using:				
	Credentials supplied by the user running				
Security	Display the following text to prompt use				
	Type or enter a user name and passwo				
	Use as Windows credentials when (
	Credentials stored securely in the report				
	User name:				
	Password:				
	Use as Windows credentials when a				
	Impersonate the authenticated user				
	 Windows integrated security 				
	Credentials are not required				
	Test Connection				
	Apply				
	7,474				

12. Remember to repeat steps 7-11 (above) for all of the reports.

You can now access the reports from either the web browser (http://localhost/Reports/browse/) or from the SCOM Console.

				– 🗆 X
(+) (-) Inttp://localhost/Reports/brov	vse/ Q - C	🚛 Home - SQL Serve	r Reporti ×	슈 ☆ 兴 (19)
SQL Server Reportin	g Services	ŝ	₹ ?	Administrator
★ Favorites 📘 Browse	C	+ ⊼ ♡	Search	م
FOLDERS (13)				
Application Monitoring	Audit Reports	•••	Microsoft.Sys lientMonitori ernal	temCenter.C *** ng.Views.Int
Microsoft.SystemCenter.D *** ataWarehouse.Report.Libr ary	Microsoft.Syst ataWarehouse	emCenter.D e.Reports	Microsoft.Sys ataWarehous el.Report.Libr	e.ServiceLev
Microsoft.SystemCenter. OperationsManager.Repo rts.2007	Microsoft.Syst WebApplicatio Library	emCenter.	My Reports	•••
ODR	Removable M Security	edia	System.Netw ment.Reports	••• orkManage
Users Folders				Ų
ح (ج) 🖉 http://localhost/Reports/browse/Removable	%20Media%20Security 🎾 🗸 🖒	<i> R</i> emovable Media Securi	ty ×	- ロ × 分☆戀 🙂
SQL Server Reporting Servi	ces		\$3 ₹	? Administrator
★ Favorites Browse	🗌 Manage folder	+ New ✔ ↑ Uploa	ad 🍸 View 🗸 Searc	ь р
Removable Media Security				
PAGINATED REPORTS (6)	••••	Domourble Modia	•••	•••
Removable Media Administration Events.rdl	movable Media All ents.rdl	Authorization Failu Events.rdl	rre Remo Chart	ovable Media s.rdl
Removable Media Online- Offline Events.rdl	•••• movable Media Write ents.rdl			

Reports - SCOMR2 - Operations Manager	
File Edit View Go Tasks Tools Help	
Search 👻 🖕 Dpen 🖕 🖡	Scope 👂 Find 😰 Tasks 😰 📮
Reporting <	Reports
 Reporting Application Monitoring Audit Reports Removable Media Security Client Monitoring Views Library Microsoft Data Warehouse Reports Microsoft Generic Report Library Microsoft Service Level Report Library Microsoft Service Level Report Library Network Management Reports Removable Media Security System Center Core Monitoring Reports Web Application Availability Monitoring Solutio Authored Reports Scheduled Reports 	 Name Removable Media Administration Events.rdl Removable Media All Events.rdl Removable Media Authorization Failure Events.rdl Removable Media Online-Offline Events.rdl Removable Media Write Events.rdl
Monitoring	
Authoring	
Reporting	

< ⊕ @	http://localhost/Reports/repo	rt/Removable%20Media%20Securi	ty/Removable%20Media%20All%20B	Events.rdl 🖉 🗢 🖒 纋 Remo	vable Media All Event ×		
SQL Se	erver Reportin	g Services					\$\$\$ ↓
★ Favorites	Browse						
Home > Re	emovable Media Secur	ity > Removable Media	All Events.rdl				
Start Date 3	/1/2019	End Date	4/1/2019				
Event Type	NLINE, OFFLINE, WRITE ST	ART. WRIT	er: SCOMR2.CONTOSO.com	~			
Userivame: C	.ONTOSO\administrator						
⊲ < [1 of 1 > ▷	I 🖒 🛞 100	∞	Find Next			
Ż	Removable Executed By: CONTOSt Execution Time: 3/8/2019 End Date: 4/1/2019 End Date: 4/1/2019 Events: 400, 403, 401, 40 Events: 400, 403, 401, 40 Computer(s): SCOMR2. Users(s): CONTOSO\ad	Media Securi D'Administrator 9 12:51:18 PM 102,600,601,300,700,701,5 810,811 CONTOSO.com ministrator	ity: All Events 00, 501, 502, 503, 504, 505, 506	, 507, 508, 509, 510, 511, 512, 513, 51	4, 515, 800, 801, 802, 803, 804,		
Event Id	Event	Time	Computer	User Name	User SID	Drive	Volume
400	ONLINE	3/6/2019 7:05:30 PM	SCOMR2.CONTOSO.com	CONTOSO\administrator		W10^E:	\Device\Har
402	WRITE COMPLETED	3/6/2019 7:06:16 PM	SCOMR2.CONTOSO.com	CONTOSO\Administrator	S-1-5-21-194330278-343332919-2867172138-500	W10^E:	\Device\Har
402	WRITE COMPLETED	3/6/2019 7:06:21 PM	SCOMR2.CONTOSO.com	CONTOSO\Administrator	5-1-5-21-194330278-343332919-2867172138-500	W10^E:	\Device\Har

SCOM and Management Pack Features

The base SCOM features combined with the SCOM secRMM Management Pack make working with secRMM very simple.

Computer Management MMC

<

If you need direct access to the secRMM MMC, you can access it directly from the SCOM console:

- 1. Click the Windows computer you want to connect to
- 2. Click the "Computer Management" link in the SCOM "Windows Computer Tasks"

San Windo	ws Computers - SC	COMR2 - Operations Manager	_ □	x			
File Edit View Go Tasks Tools Help							
Search 👻 🛫 👬 Scope 🔎 Find 🖸 Tasks 🔞 👙							
Monitoring <	Windows Computers	(2)	 Tasks 				
4 Monitoring	🔍 Look for:						
Active Alerts	State 🔺 🖉	Name	Windows Computer Tasks	^			
Distributed Applications	🕢 Healthy	SCOMR2.CONTOSO.com	Computer Management				
Task Status		WORKSTATIONA.CONTOSO.com	Ping Computer				
Windows Computers			Ping Computer (with Route)				
Agentless Exception Monitoring	< 111	>	Ping Computer Continuously (pi	ing -t)			
Application Monitoring	Detail View	~	Remote Desktop				

*	Computer Manager	nent	
File Action View Help			
E Computer Management (WORKSTATIONA.CONTOSO.COM)	Computer Configuration		
⊿ 🙀 System Tools	Name	Value	~
Task Scheduler Task Scheduler	AllowedDirectories	C:\Users\ <userid>;\\UserShare</userid>	
Event Viewer	AllowedFileExtensions		
secRMM (WORKSTATIONA.CONTOSO.com)	AllowedInternalIds		
ki Shared Folders	AllowedPrograms		
Local Users and Groups	AllowedSerialNumbers		
Performance	AllowedUsers		
🚑 Device Manager	FailWritelfSourceFileUnknown	on	
	InstallDateTime	N9/N2/2012 19/N1/27	

SCOM secRMM Tasks

The secRMM Management Pack includes SCOM Tasks which allow you to perform certain common secRMM functions directly within the console. As an example, the screen shots below show how the SCOM operator can act as the "secRMM SafeCopy Approver" (i.e. enforceable two man policy). The first screen shot shows how an alert gets generated when the end-user starts the secRMM SafeCopy program to write to a removable media device. The SCOM operator can click that alert and then click the SCOM "secRMM SafeCopy Approver" task to approve or reject the end-users request (screen shot

2).							
		Removable Media Alerts	- SCOMR2 - O	perations Manager			_ D X
File Edit View Go Tasks Tools Help							
Search 👻 🝦 Överrides 👻	🝦 🌆 Scope 🔎 Fin	d 🚺 Tasks 🔞 🖕					
Monitoring <	Removable Media Aler	ts (5)					Tasks
4 🔳 Monitoring	🔍 Look for:		Find Now	Clear			
Active Alerts	Severity 🚯 Icon	Path	Name		Source	Ore ^	Alert Actions
Discovered Inventory	Information (1)	WORKSTATIONA.CONTOSO.com	secRMM SafeCop	oy PreApproval	Squadra.secRMM.Event	12/	
Task Status	Warning 🛕	WORKSTATIONA.CONTOSO.com	Property Change	d - secRMM	Squadra.secRMM.Event	12/ 🗸	Subscription V
UNIX/Linux Computers	<					>	Tasks 🗸
Windows Computers	Alert Details					~	Navigation 🗸
Agentless Exception Monitoring	() corDMM SafeCo	ny Dra Annroual		Alart Description		~	
Application Monitoring	Seckivitvi SaleCo	ру гедррома		Alert Description			secRMM Tasks
A Microsoft Audit Collection Services	Source: 🔯 S	Squadra.secRMM.Event		Event Description: Removal User is requesting approva	ole Media Security Application I to use secRMM SafeCopy		Authorize Internal Ids
Microsoft Windows Client	Alert Rule:	ecRMM SafeCopy PreApproval	ra.seckiviivi.event	User: WorkstationA\Admini	strator		Authorize Programs
Microsoft Windows Server	Created: 1	12/28/2013 1:34:05 PM		Program: C:\Program			Authorize Serial Numbers
Network Monitoring				Files/seckivilvi/oserotiis/sec	Rivinisarecopy.exe, PiD: 2556		Authorize Users
Operations Manager							secRMM Lockdown mode
Synthetic Transaction	Knowledge:			/iew additional knowledge			secRMM Monitoring mode
UNIX/Linux Computers	No knowledge was ava	ailable for this alert.					secRMM SafeCopy Approver
Web Application Transaction Monitoring	Hide knowledge						Demonst Textus
4 🙀 Windows Service And Process Monitoring							керогт тазкз 🗸 🗸
Process State							
Removable Media Alerts							
Windows Service State							

Removable N	edia Alerts (5)	
🔍 Look for:		Find Now Clear
Severity	🚯 Icon Path	Name
Information	WORKSTATIONA.CONTOSO.com	secRMM SafeCopy PreApproval
Warning	WORKSTATIONA.CONTOSO.com	Property Changed - secRMM
46	secRMM SafeCopy Appro	ver 🗕 🗖 🗙
Connect WORKS User: Program: PID:	ed to computer: TATIONA Connect WorkstationA\Administrator C:\Program Files\secRMM\UserUtils\secRMMSafe 2556	Help tion otion: Remova esting approva ationA\Admir Program A\UserUtils\se
	Accept Reject Put secRMM in Lockdown mode when user ex Require approval on copy operations	I knowledge. ots SafeCopy

When you run the secRMM Operations Manager agent tasks, be sure that you specify an Administrator userid to run the task if the Operations Manager agent is not a member of the local Administrators group (see screenshot below). If the Operations Manager is a member of the local Administrators group on the Windows computer where you will be running the agent task, then you do not need to specify a different userid.

Run the <u>t</u> ask on these target	ts	
Target	Run Location	
☑ Squadra.secRMM.Event	w200364.mms.com	
T <u>a</u> sk Parameters		
Name		Valu
Arguments		Null
<u>O</u> verride		
ask credentials		
ask credentials	ccount	
ask credentials C Use the predefined Run As A O Oth <u>e</u> r :	ccount	
ask credentials C Use the predefined Run As A ● Other : <u>U</u> ser name : Administrator	ccount	

By default, the secRMM Operations Manager agent tasks are setup to clear each secRMM property (that is AllowedUsers, AllowedPrograms and AllowedSerialNumbers). If you want to use the secRMM Operations Manager agent tasks to set one of the secRMM authorization properties, you need to override the task parameter from with the Operations Manager Console (please see the screenshots below).

arget		Run L	Location			
Squadra.secRN	MM.Even	t w200	364.mms.com			
sk Parameters	:					
ame				Value		
imeout Seconds				60		
arguments				Null		
<u>O</u> verride						
Override				Task descrip	ion.	
Override				Task descript	tion	
Override	ameter	5		Task descript	tion	
Override k credentials verride Task Par	'ameter: paramet	s ers with the	e new values	Task descript	tion	
Override sk credentials verride Task Par erride the t <u>a</u> sk p	'ameter: paramet	s ers with the Default Value	e new values New Value	Task descript	tion	
Override k credentials rerride Task Par erride the task p Name Timeout Seconds	rameters paramet Type int	s ers with the Default Value 60	e new values New Value	Task descript	tion	

You can verify the secRMM Operations Manager agent task by viewing the task status view from with the Operations Manager Console.

Systen	n Center Opera	tions Ma	nager 200	7 R2 - QST						
<u>F</u> ile <u>E</u>	dit <u>V</u> iew <u>G</u> o	o <u>A</u> ction	s <u>T</u> ools	<u>H</u> elp						
		earch 🔹	Scope	Eind 😫 Ad	tions 0					
Monito	pring	Lask	Status	; (2)						
🖃 🜉 Ma	onitoring	<u>L</u> oc	k for:			Eind Now	⊆lear			
	Active Alerts	Status		Task Name	Schedule Time		Start Time	∇	Submitted By	Run As
	Distributed Applic	ia 🕢 Sua	cess	Authorize Users	3/24/2011 12:15	:32 PM	3/24/2011 1	12:15:35 PM	W200364\Admin	W200364\Admir
2	Task Status	Ĭ					-11			
	Unix/Linux Serv	e Detaile								
	Windows Comp	ul Decails								
+ 4	Agentless Exce Microsoft Audit	. 🕗	Authorize	Jsers				Task	Description	
± 📮	Network Device	Status	5:		Success			This o	psmgr agent task allo	ws you to set th
+ 📮	Operations Man	a Sched	uled Time:		3/24/2011 12:15:3	2 PM		secRM	1M AllowedUsers prop	perty tells secRMI
+ 📴	Synthetic Trans	a Start i	Time:		3/24/2011 12:15:3	5 PM		compl	vable Media Device. etelv disallow use of I	The secrimim Alloy Removable Media
+ 📴	Web Application	י Submi	tted By:		W200364\Administ	rator		value	that will never match	any userid within
E 🔄	Windows Servic	Run A	s:		W200364\Administ	rator		secRM	1M AllowedUsers prop	perty is a semicole
	Process Sta	Run L	ocation:		w200364.mms.con	1		or the	e userias is domainivai	nețuseria
	Kemovable	M Targe	t:		Squadra.secRMM.I	Event				
	windows 5	Targe	t Type:		secRMM					
		Categ	ory:		Security Health					
		Task	Output:							
		Out sec Erro Non	put RMM Prop r e	erty AllowedUs	sers has been :	set	_	_		
		Exit	Code: 0							

Available Reports

There are 5 secRMM reports available:

- 1. All secRMM events
- 2. Administration events
- 3. Authorization Failure events
- 4. Online/Offline events
- 5. Write events

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, Windows 8, Windows 2012, etc.
- 3. The version of SCOM you have installed.
- 4. Whether the Windows Operating System is 32bit or 64bit.
- 5. 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/