Security Removable Media Manager

SCOM 2012

Administrator Guide

Version 9.9.13.0

(May 2019)

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

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

Introduction

Security **R**emovable **M**edia **M**anager (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

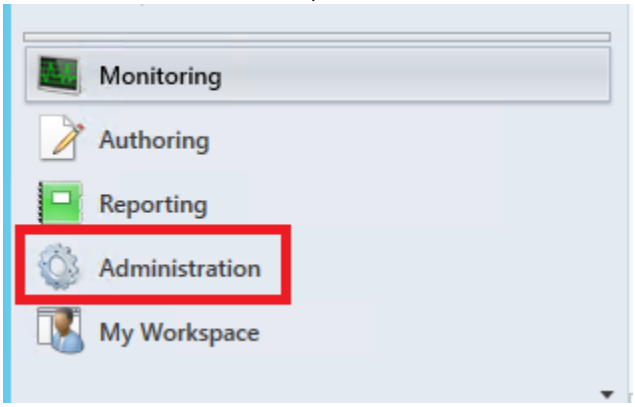
Install the secRMM SCOM Management Pack

1. Download the secRMM Management Pack from the Squadra Technologies web site at http://www.squadratechnologies.com/Products/secRMM/SystemCenter/secRMMSystemCenterOperationsManager.aspx 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.

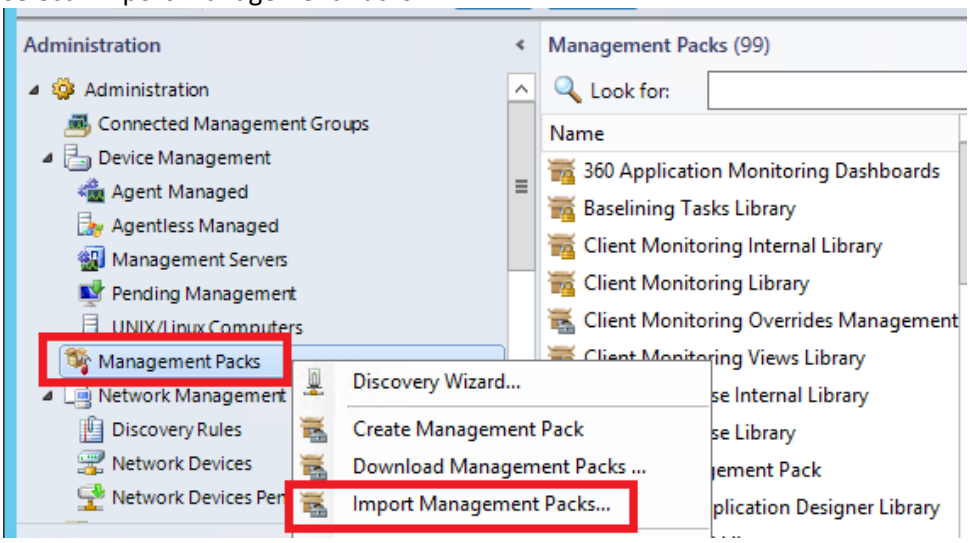
   Please note that if you use the secRMMCentral Management Pack, the computer with secRMMCentral running on it **MUST** also have secRMM installed on it as well. Failure to have secRMM installed will result in invalid event data getting inserted into the SCOM database and this will then cause the secRMM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

2. Open the SCOM Console using a userid that is a SCOM Administrator.

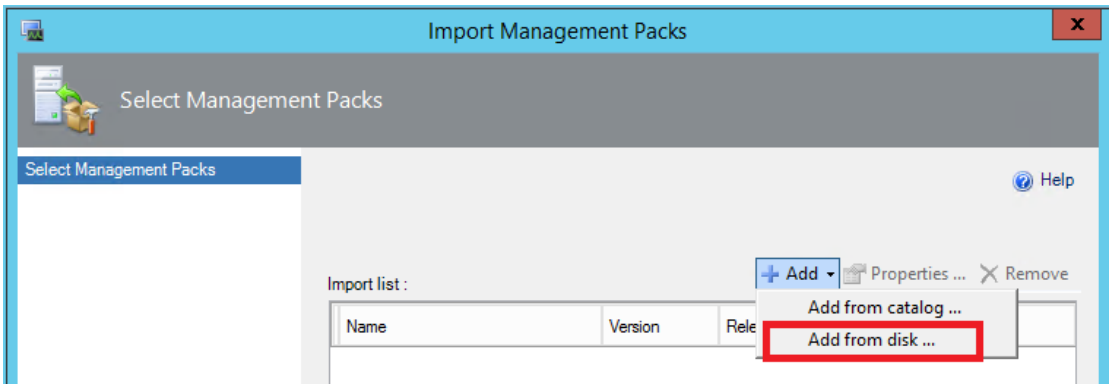
3. Within the SCOM Console, select "Administration" view



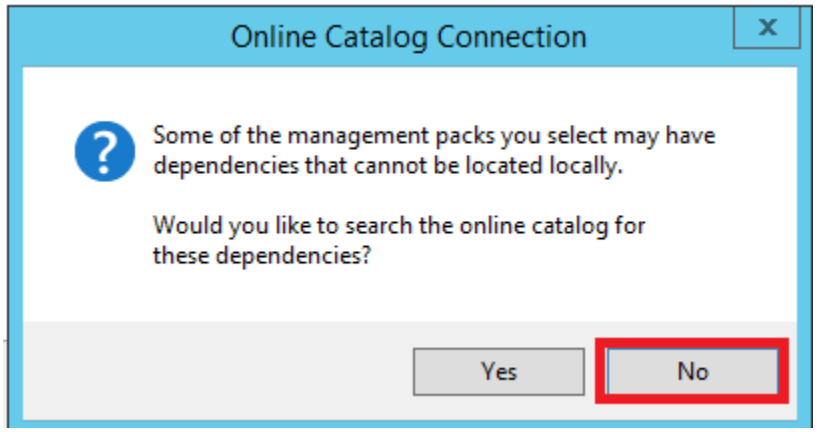
4. In the Administration view, right mouse click on “Management Packs”. From the pop-up menu, select “Import Management Packs…”



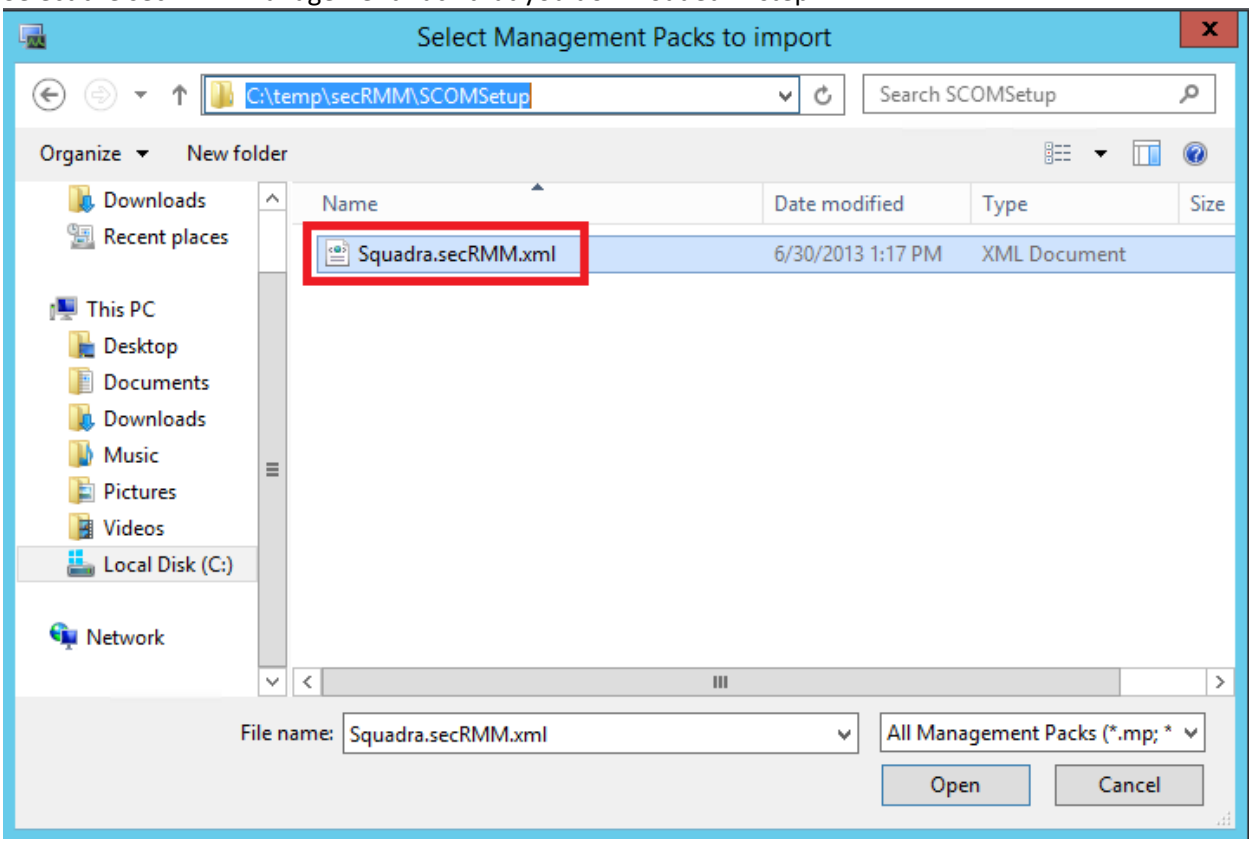
5. In the “Import Management Packs” dialog, click the Add drop-down button and then select “Add from disk…”.



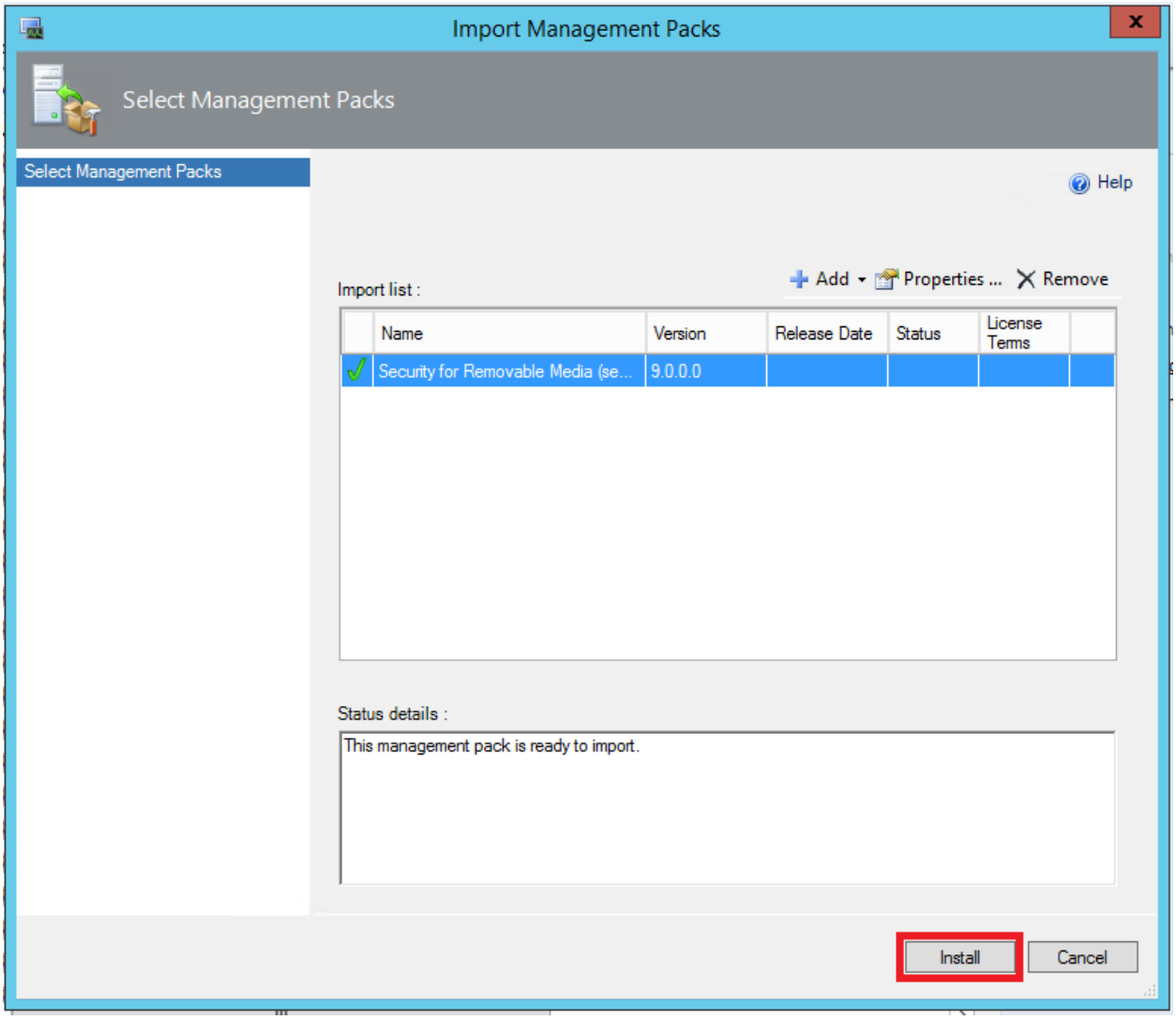
6. Select “No” when the “Online Catalog Connection” message box appears.



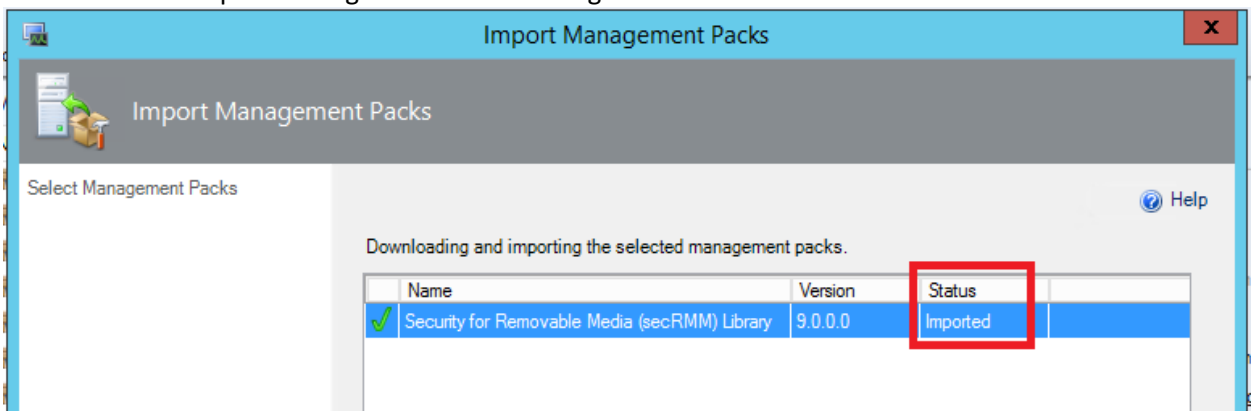
7. Select the secRMM Management Pack that you downloaded in step 1.



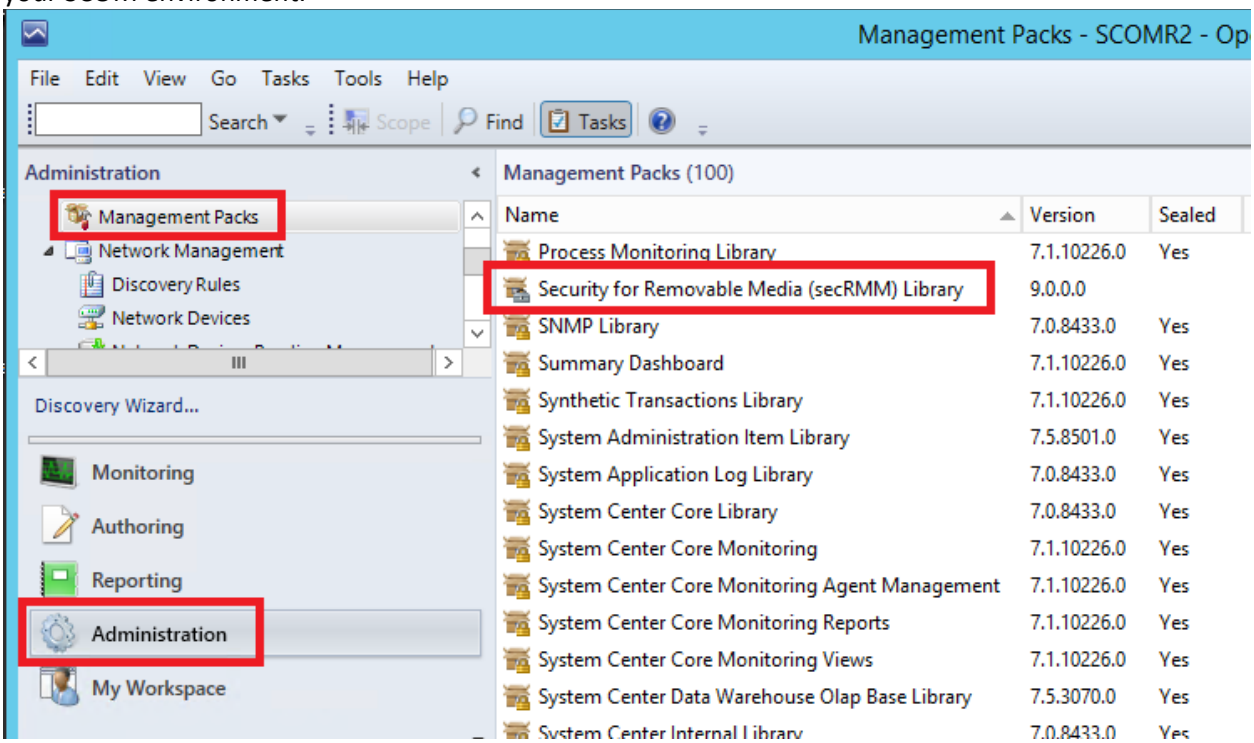
8. Click the “Install” button.



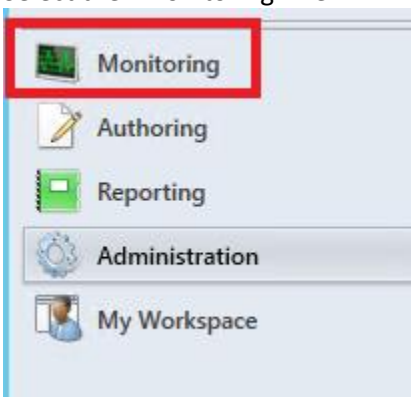
9. When the import completes, you will see a status of "Imported". Click the "Close" button at the bottom of the "Import Management Packs" dialog.



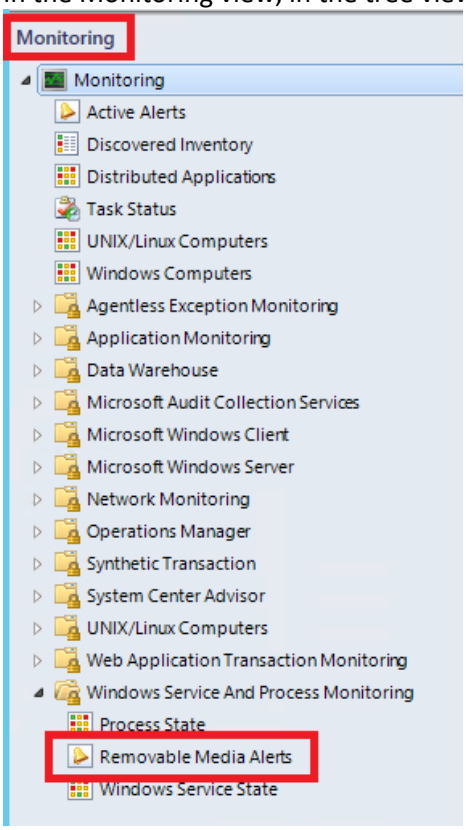
10. From the Administration view, you will see the secRMM Management Pack in the list of "Management Packs". You may need to hit refresh several times depending on the workload of your SCOM environment.



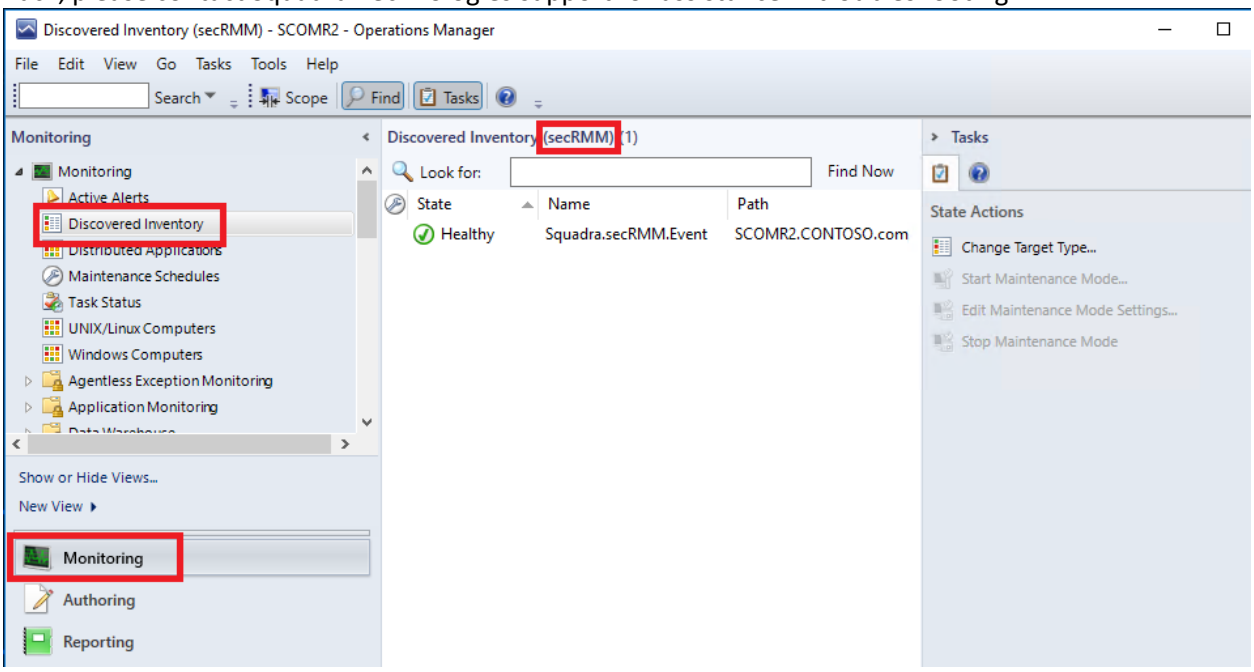
11. Select the “Monitoring” view



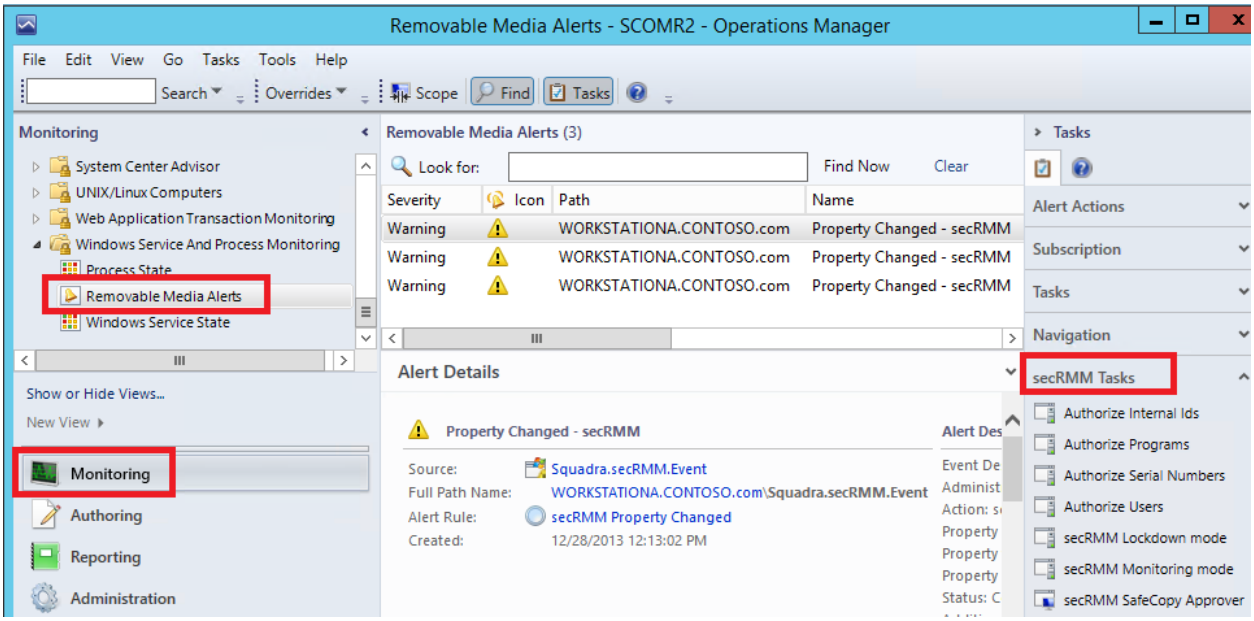
12. In the Monitoring view, in the tree view section, you will see the “Removable Media Alerts” view



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.



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.

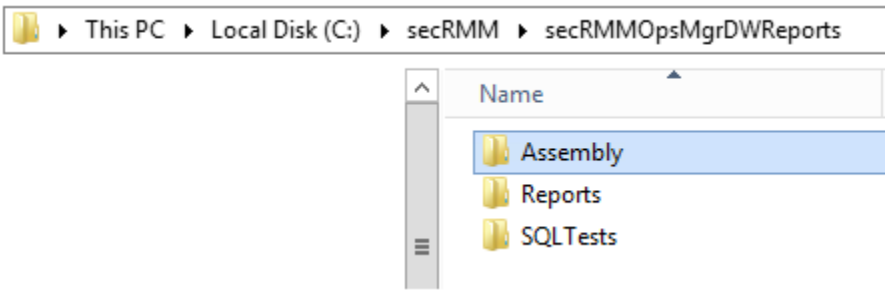


Install the secRMM SCOM Reports

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 http://www.squadratechnologies.com/Products/secRMM/secRMMReports.aspx. 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.

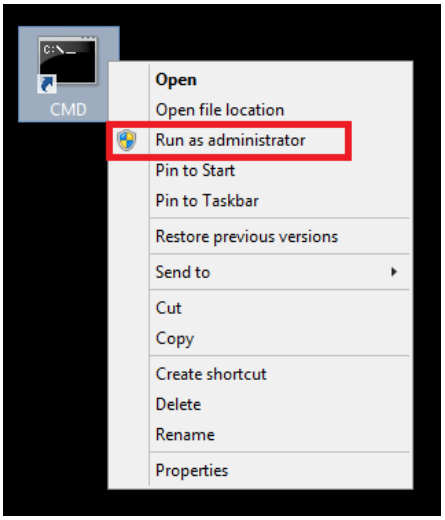
The unzipped folder will have three subfolders in it: Assembly, Reports and SQLTests.



Register the secRMM .Net assembly into SQL

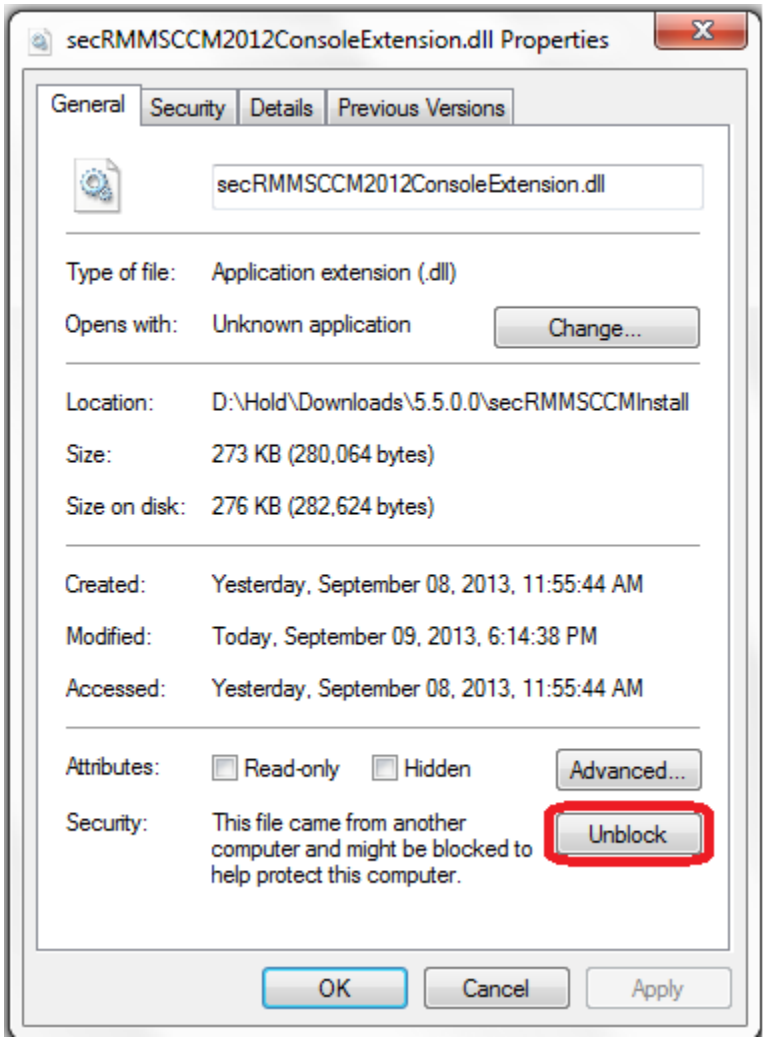
The process of registering the secRMM .Net assembly is the same whether you are performing the step for the SCOM DW or the SCOM AC data base.

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

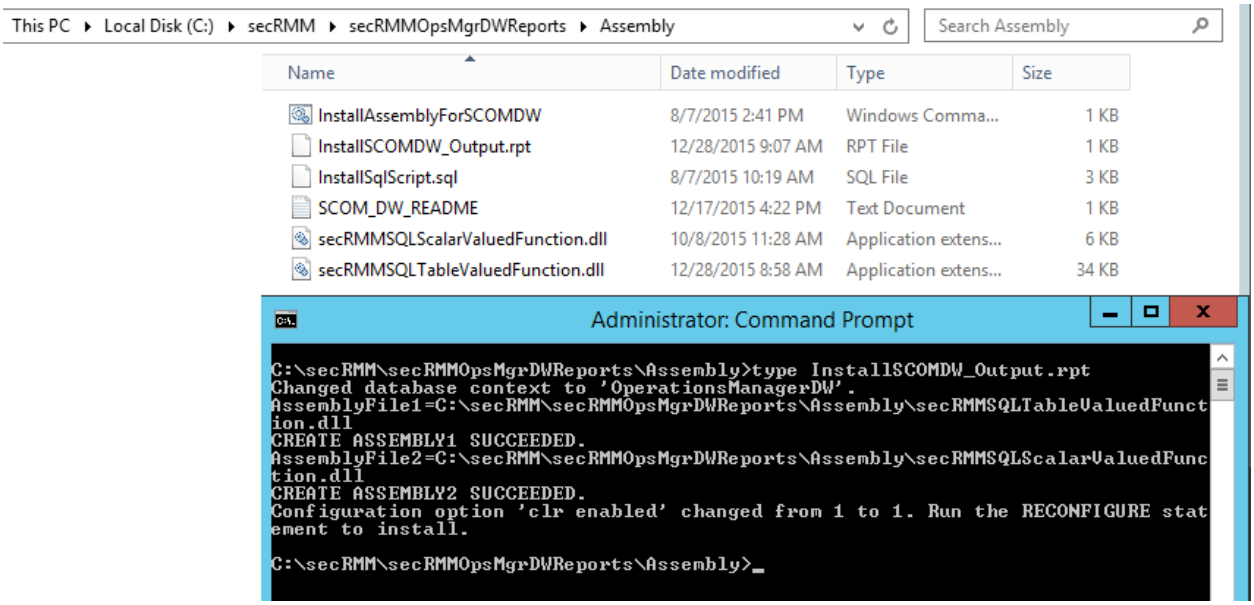


2. Go to the directory where you extracted the **secRMMOpsMgrDWReports.zip** or **secRMMOpsMgrACSReports.zip** file. Go into the Assembly subfolder.

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.



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.

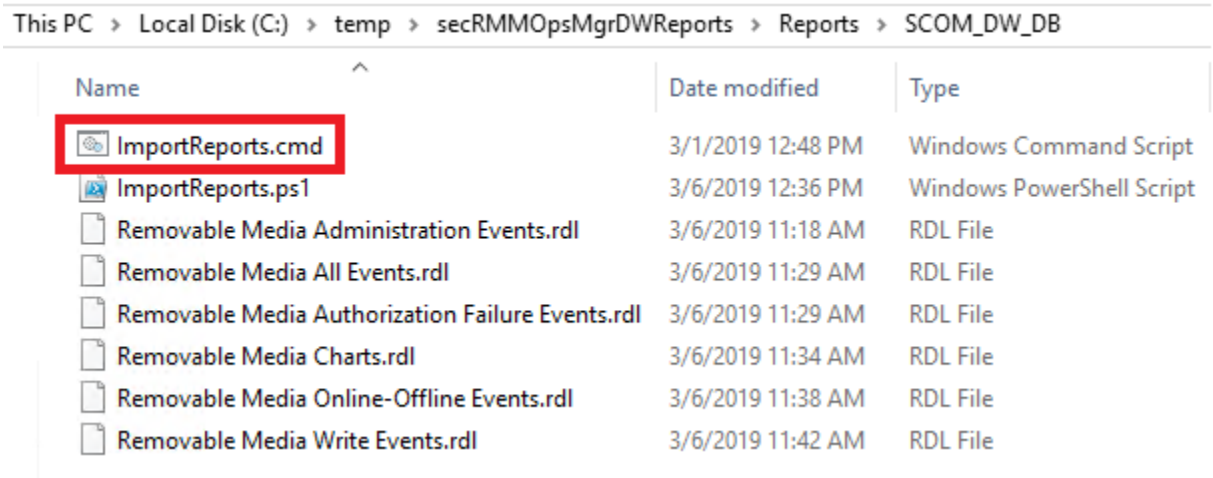

This PC ▸ Local Disk (C:) ▸ secRMM ▸ secRMMOpsMgrDWReports ▸ Assembly
Search Assembly
Name
Date modified
Type
Size
InstallAssemblyForSCOMDW 8/7/2015 2:41 PM Windows Comma... 1 KB
InstallSCOMDW_Output.rpt 12/28/2015 9:07 AM RPT File 1 KB
InstallSqlScript.sql 8/7/2015 10:19 AM SQL File 3 KB
SCOM_DW_README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

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

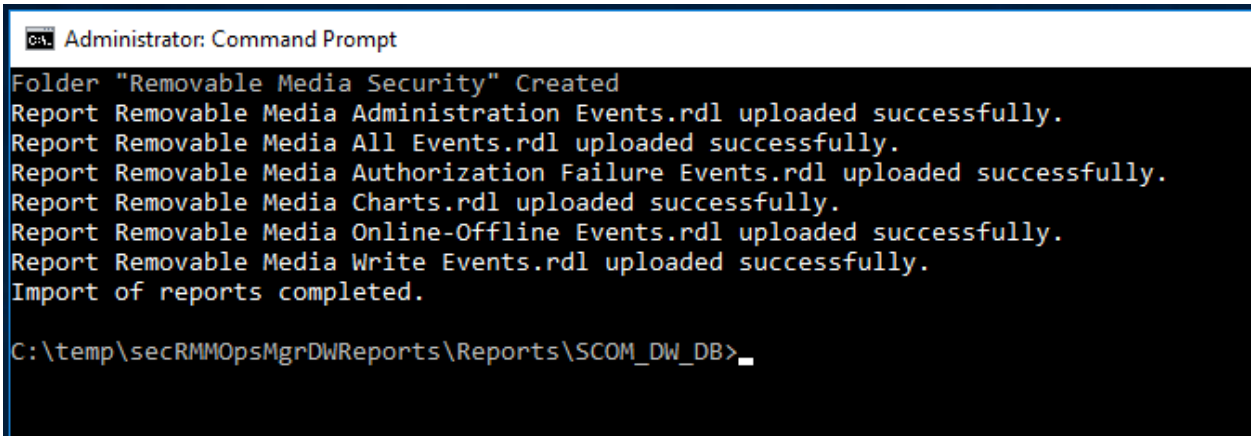
Load secRMM reports into SSRS using Powershell

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).



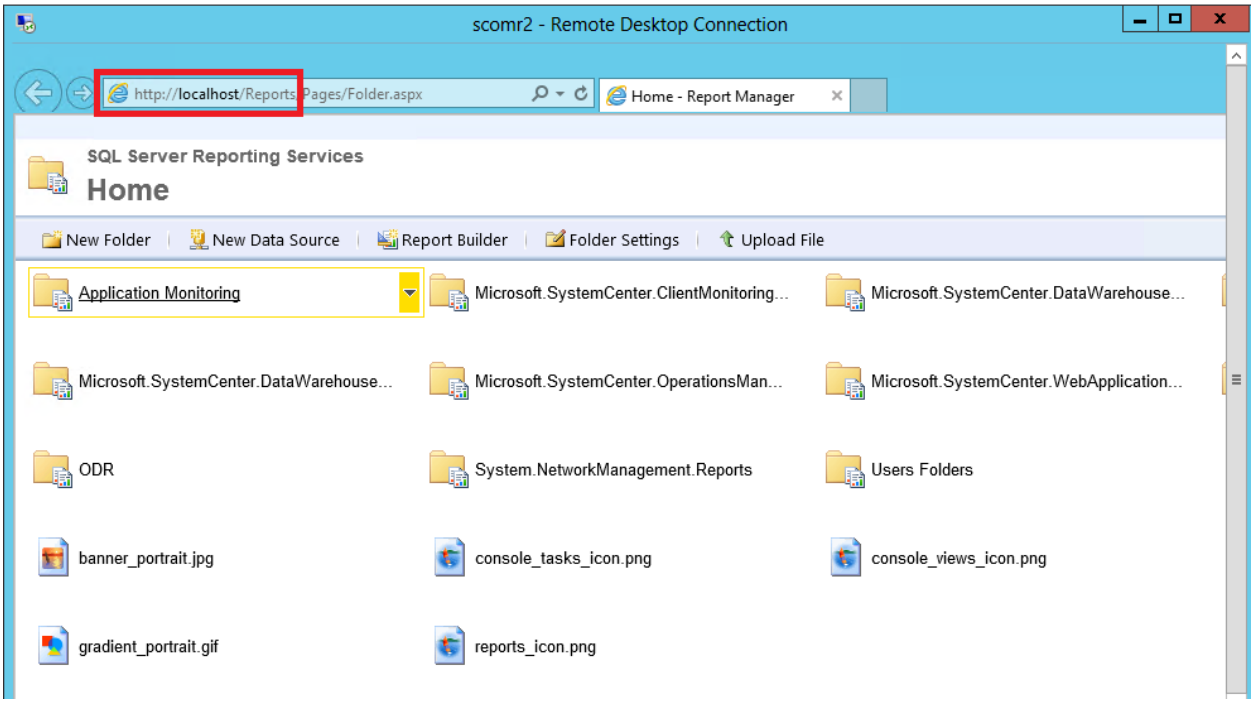
4. In the command window, type ImportReports.cmd and hit the enter key.
   The output will look similar to the screenshot below.



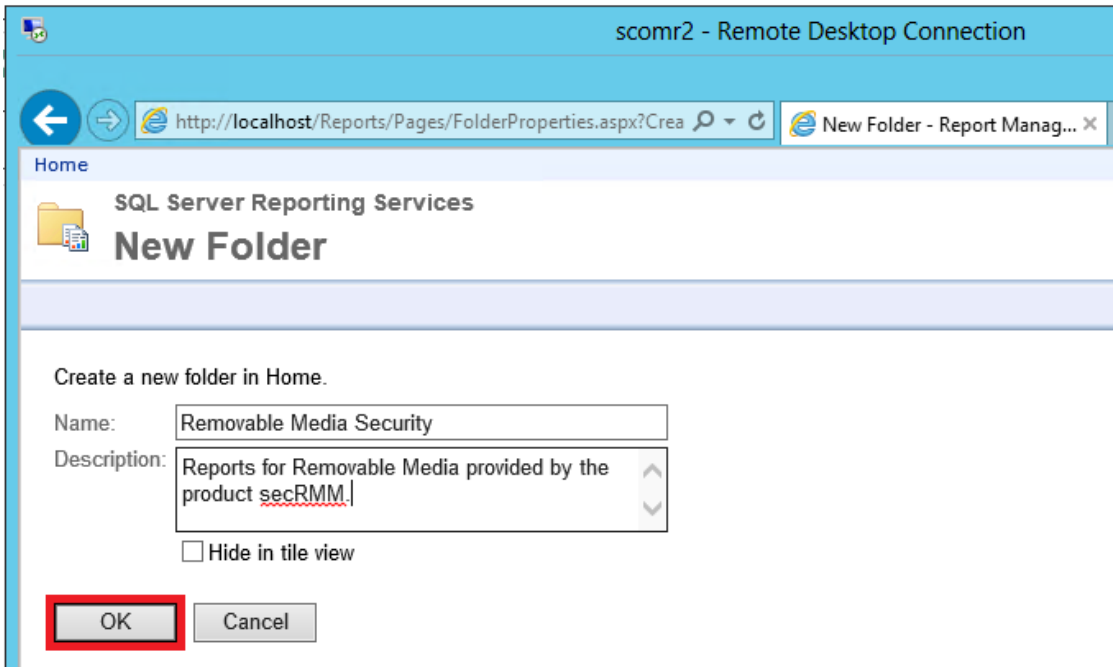
If the Powershell output looks like the above screenshot, you may skip over the "Load secRMM reports into SSRS manually" subsection below.

Load secRMM reports into SSRS manually

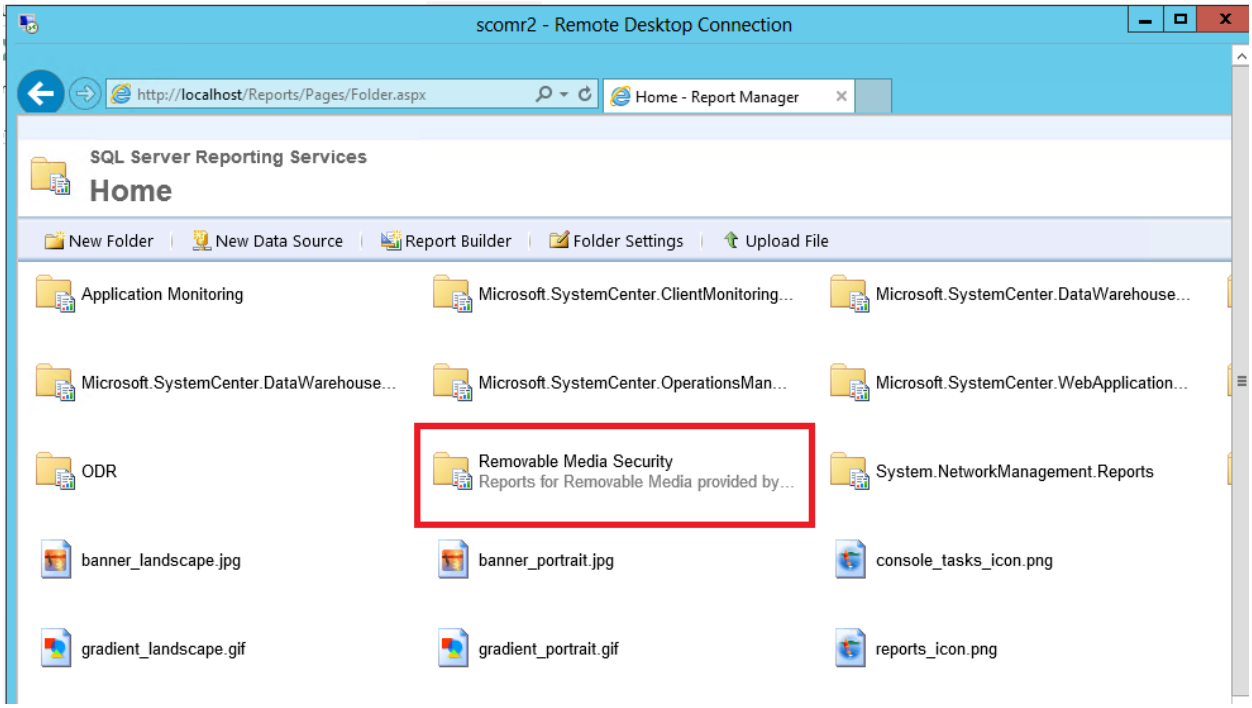
1. On the Windows computer where SSRS is running, open a web browser and go to the URL http://localhost/reports.


scomr2 - Remote Desktop Connection
http://localhost/Reports/Pages/Folder.aspx
Home - Report Manager
SQL Server Reporting Services
Home
New Folder
New Data Source
Report Builder
Folder Settings
Upload File
Application Monitoring
Microsoft.SystemCenter.ClientMonitoring...
Microsoft.SystemCenter.DataWarehouse...
Microsoft.SystemCenter.DataWarehouse...
Microsoft.SystemCenter.OperationsMan...
Microsoft.SystemCenter.WebApplication...
ODR
System.NetworkManagement.Reports
Users Folders
banner_portrait.jpg
console_tasks_icon.png
console_views_icon.png
gradient_portrait.gif
reports_icon.png

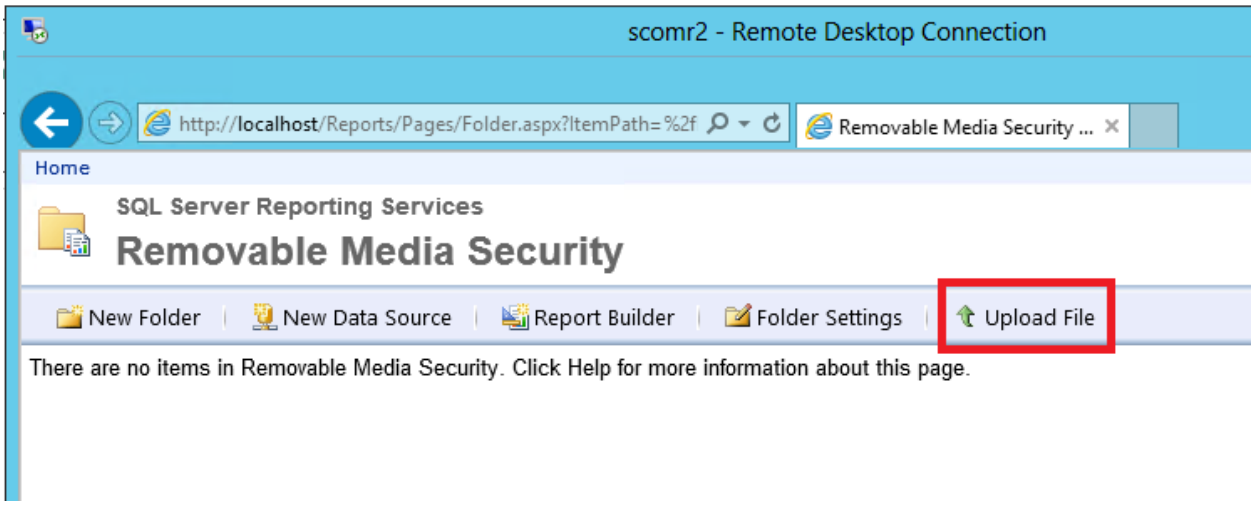
2. Select the “New Folder” option and create a folder named “Removable Media Security”



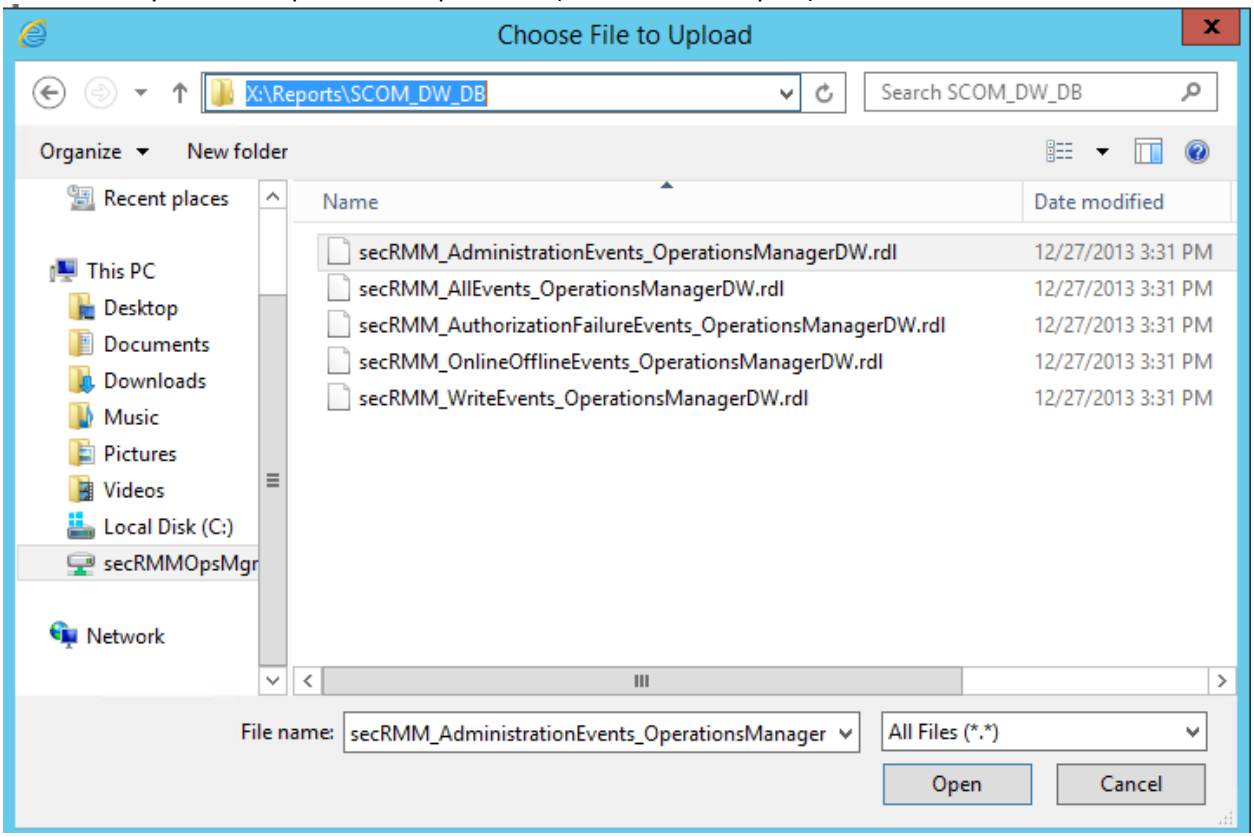
3. You will see the new folder on the main page. Double click the new folder to go into it.

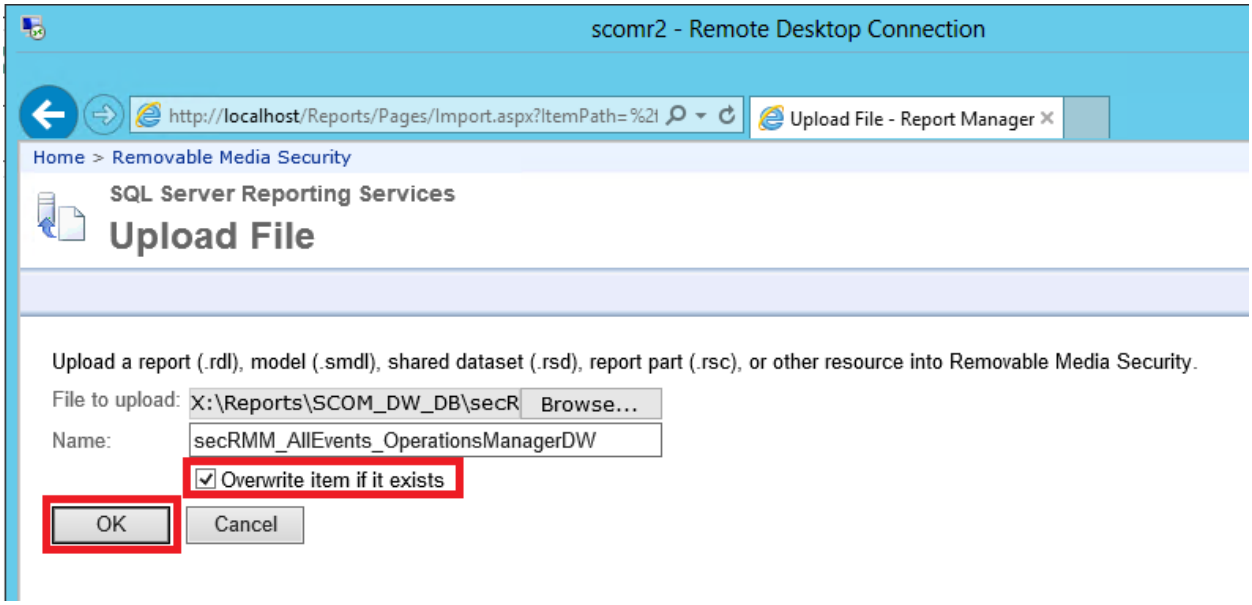


4. Select the “Upload File” option

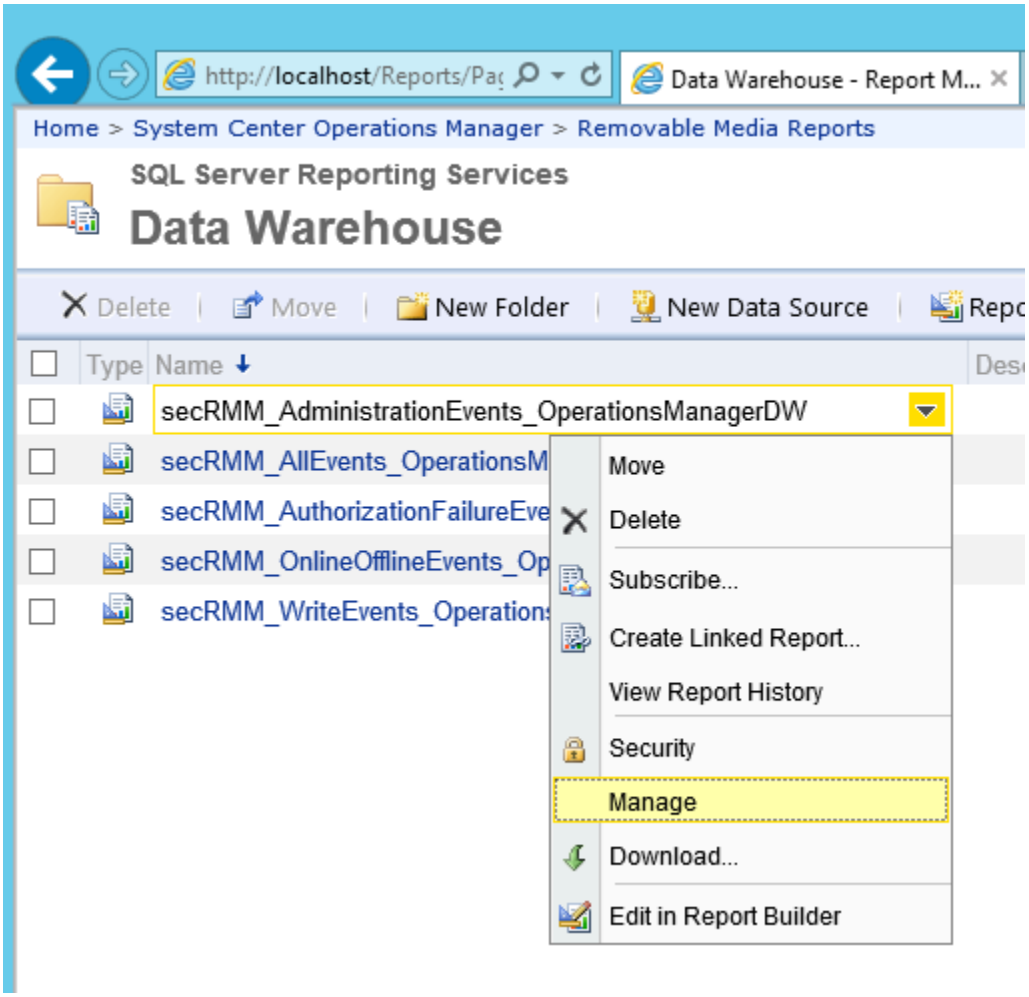


5. From the “Choose File to Upload”, go to the SCOM_DW_DB or SCOM_AC_DB folder (under the directory where you extracted the **secRMMOpsMgrDWReports.zip** or **secRMMOpsMgrACSReports.zip** file) depending on which SCOM database you are importing the reports for. Unfortunately, the “Choose File to Upload” dialog only allows you to choose one file at a time so you must repeat this step 5 times (once for each report).

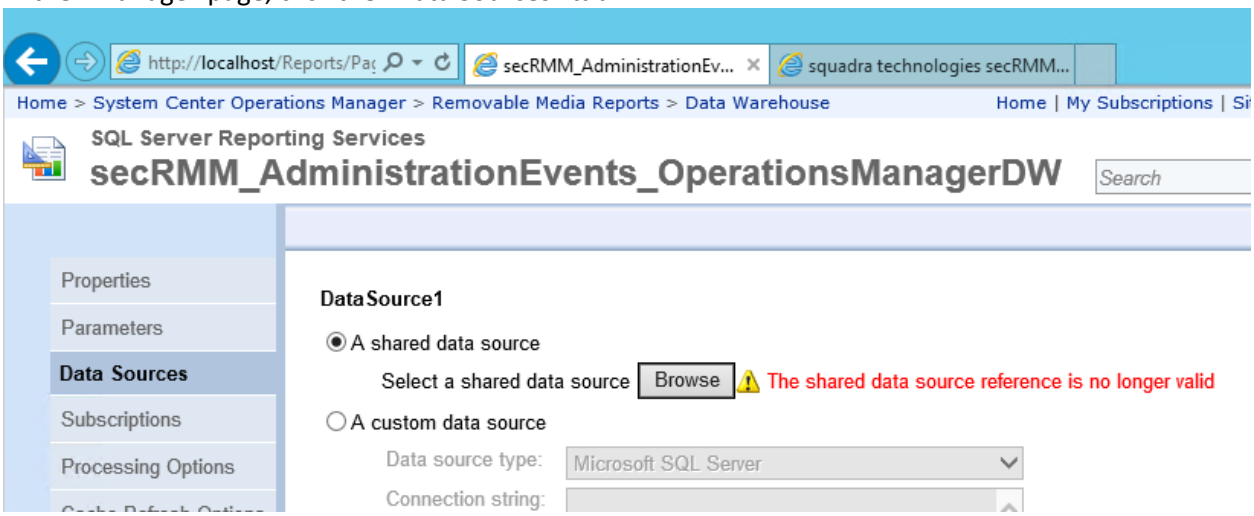




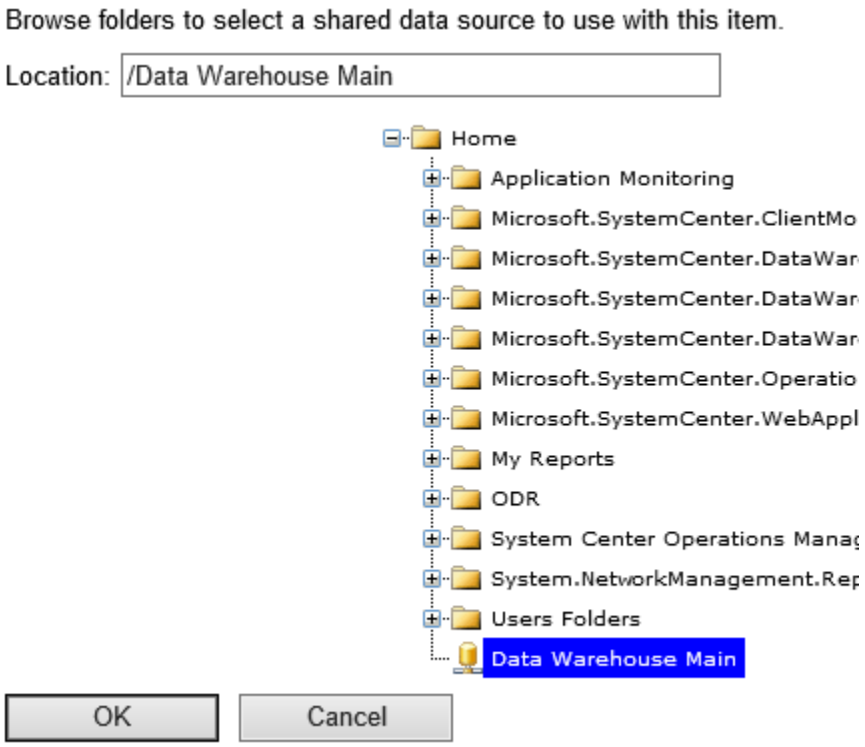
6. When you are finished with the uploads, you will have all the secRMM reports loaded. The last step is to associate the SCOM SQL datasource to each report. Unfortunately, you must repeat the following steps for each report since there is no way to apply it to all the reports at one time.
7. To the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



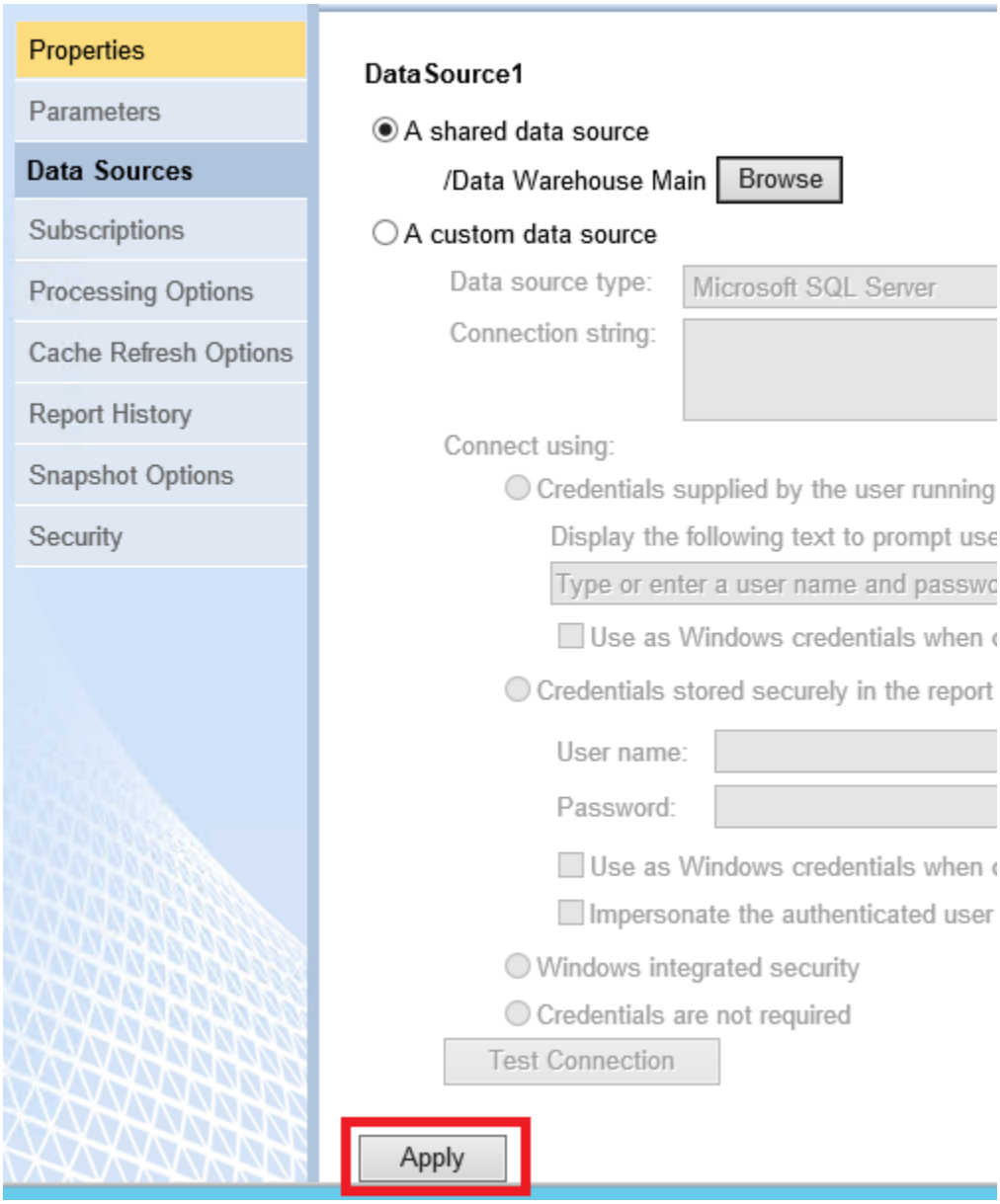
8. In the “Manage” page, click the “Data Sources” tab.



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

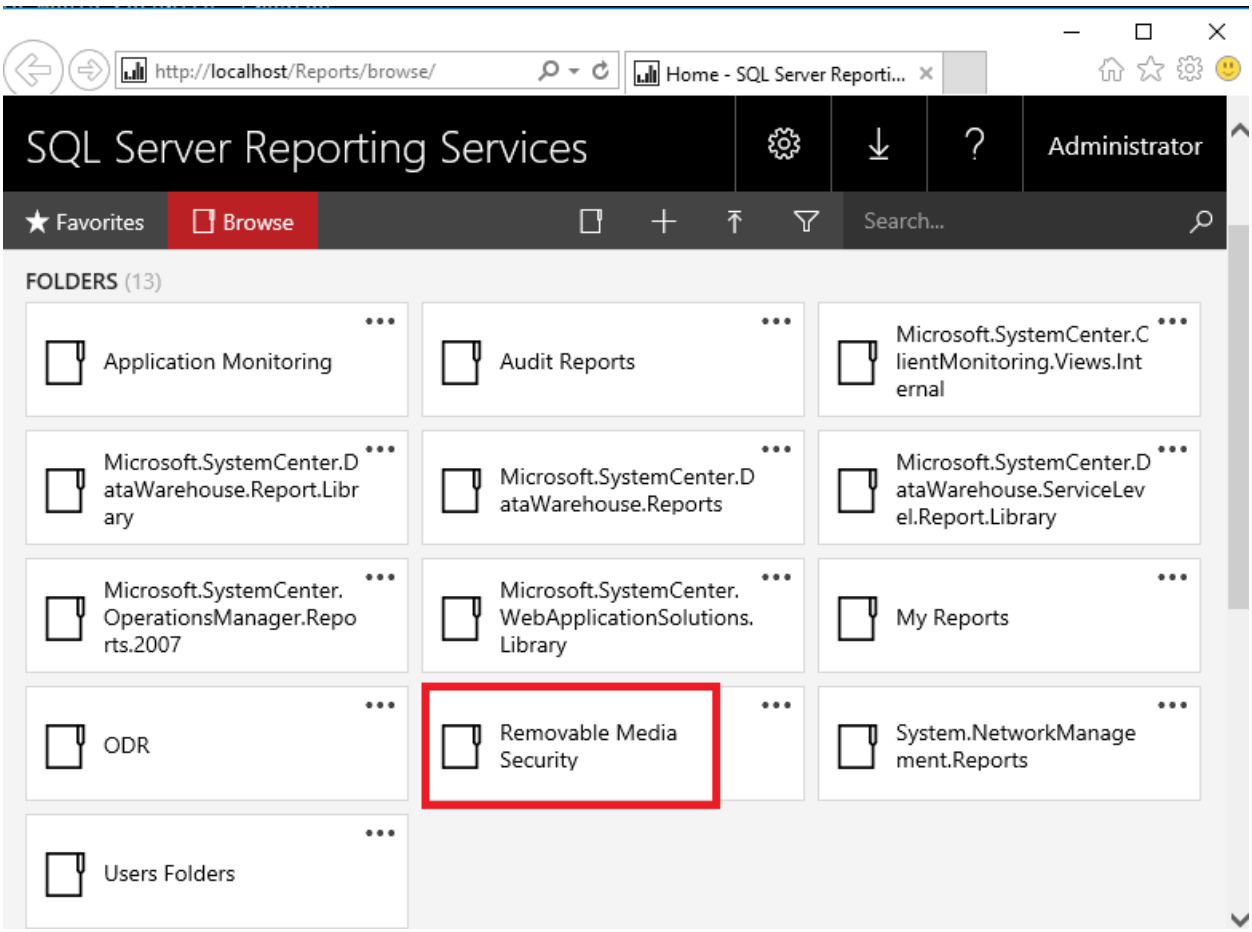


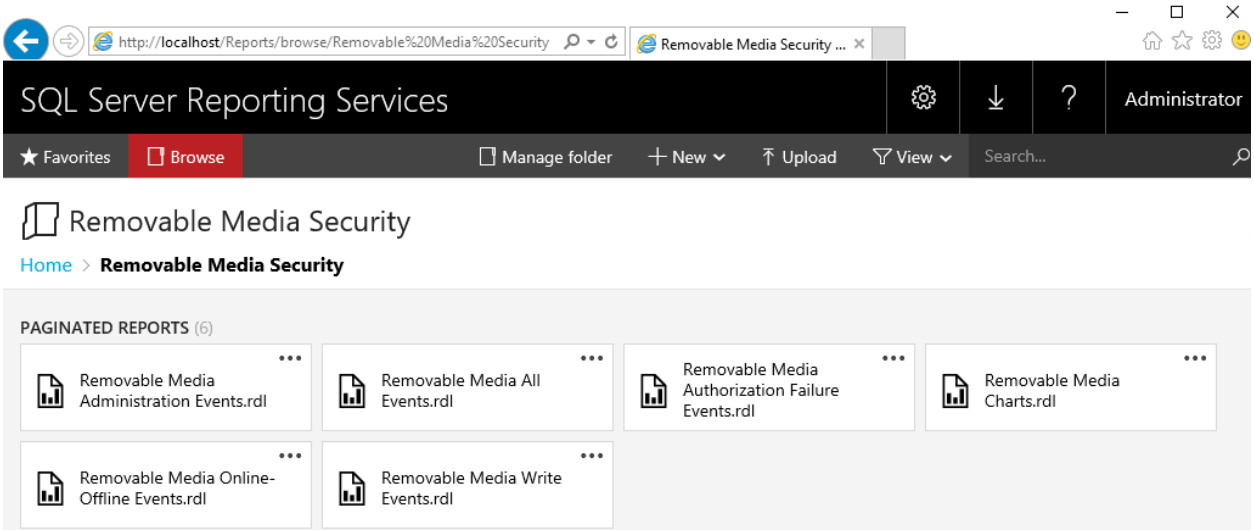
10. Click the “Data Warehouse Main” or “Audit and Collection Services” data source (it should be at the very bottom of the list) and then click OK.
11. You will now be back on the “Manage”->”Data Sources” page. Make sure you click the “Apply” button on the bottom of the page.

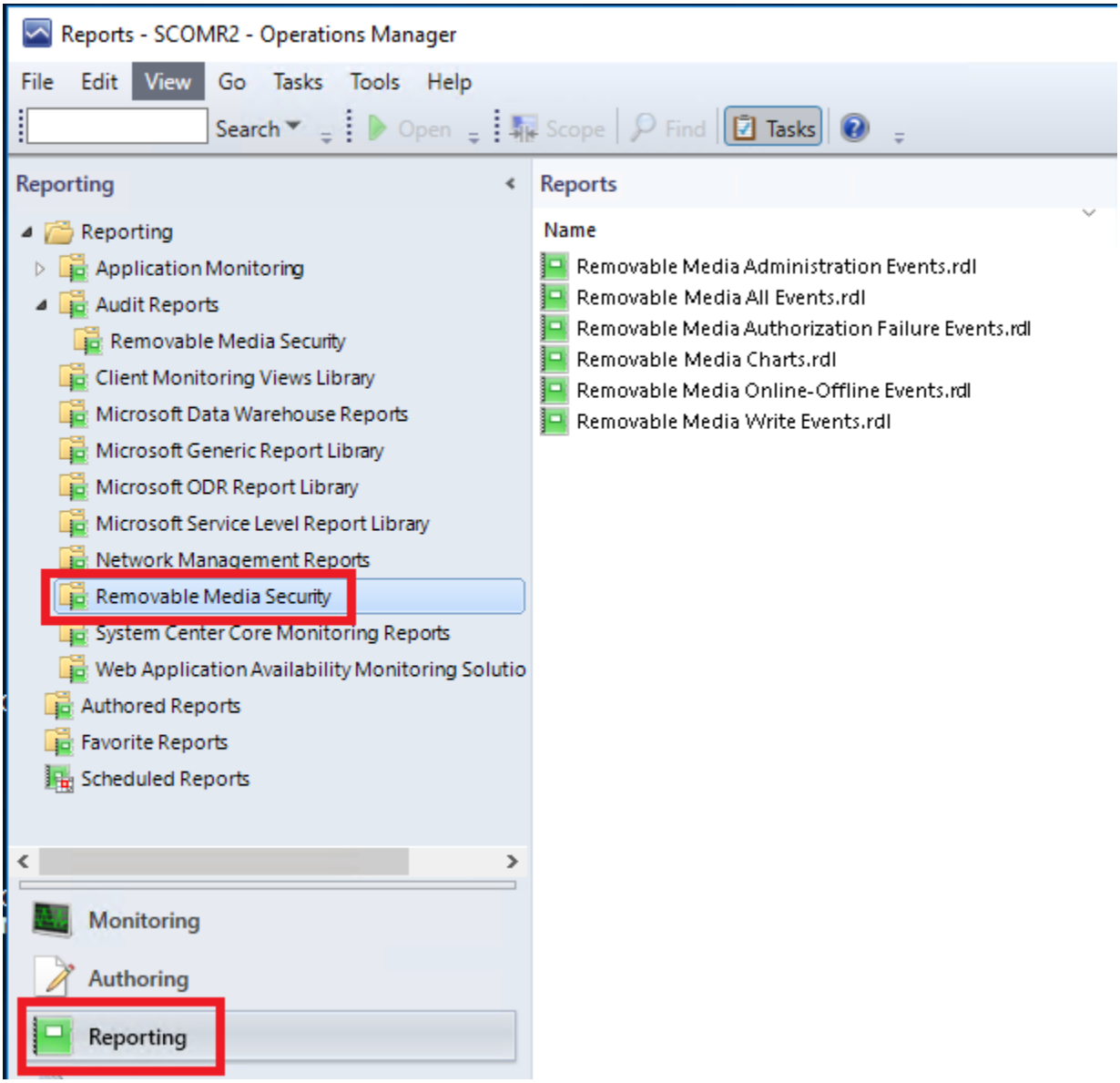


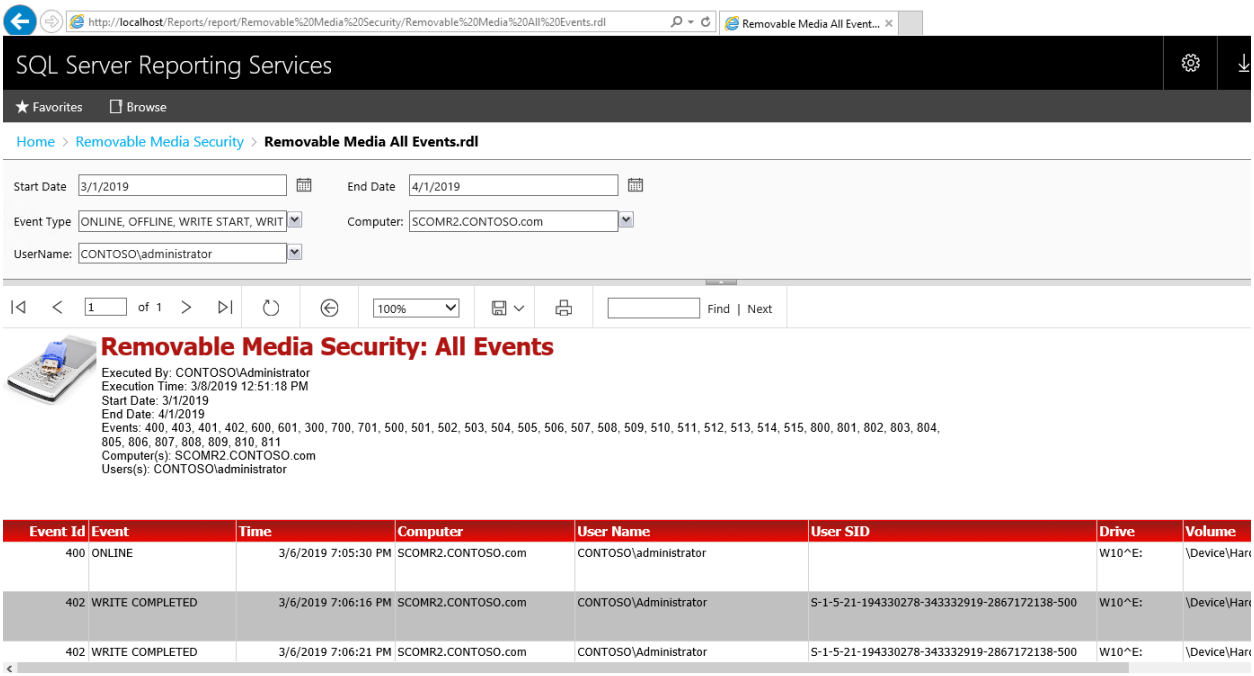
12. Remember to repeat steps 7-11 (above) for all of the reports.

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






Reports - SCOMR2 - Operations Manager
File
Edit
View
Go
Tasks
Tools
Help
Search
Open
Scope
Find
Tasks
Reporting
Reporting
Application Monitoring
Audit Reports
Removable Media Security
Client Monitoring Views Library
Microsoft Data Warehouse Reports
Microsoft Generic Report Library
Microsoft ODR 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
Favorite Reports
Scheduled Reports
Monitoring
Authoring
Reporting
Reports
Name
Removable Media Administration Events.rdl
Removable Media All Events.rdl
Removable Media Authorization Failure Events.rdl
Removable Media Charts.rdl
Removable Media Online-Offline Events.rdl
Removable Media Write Events.rdl



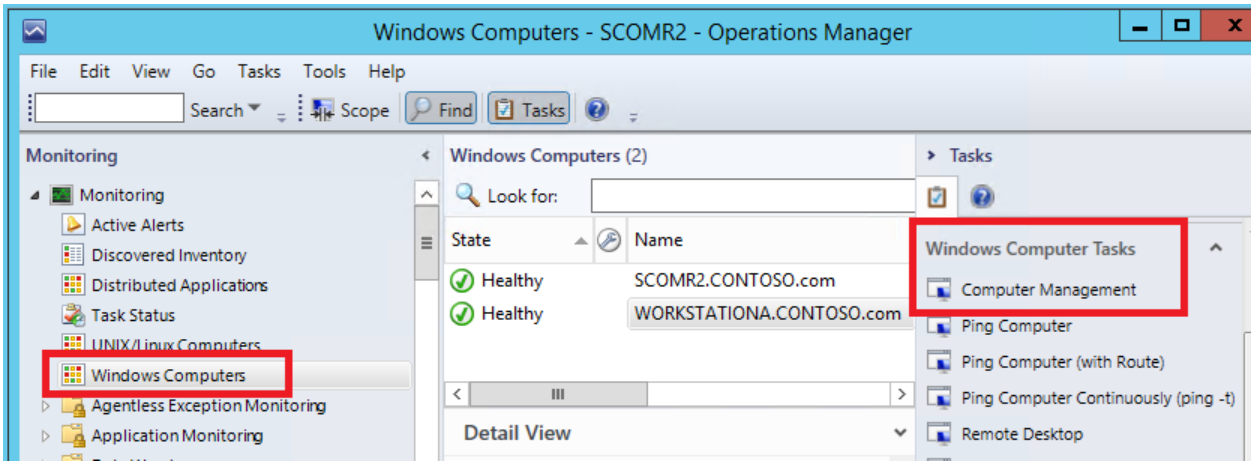
SCOM and Management Pack Features

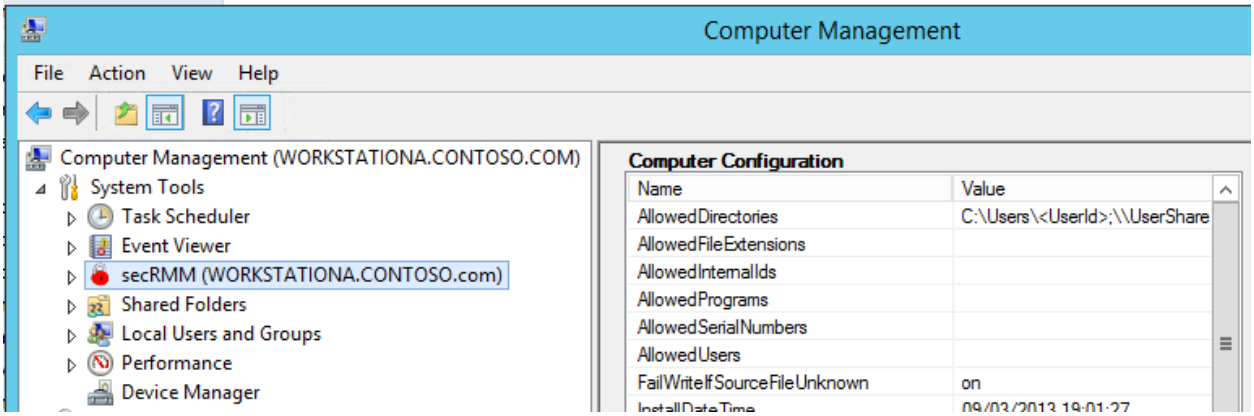
The base SCOM features combined with the SCOM secRMM Management Pack make working with secRMM very simple.

Computer Management MMC

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

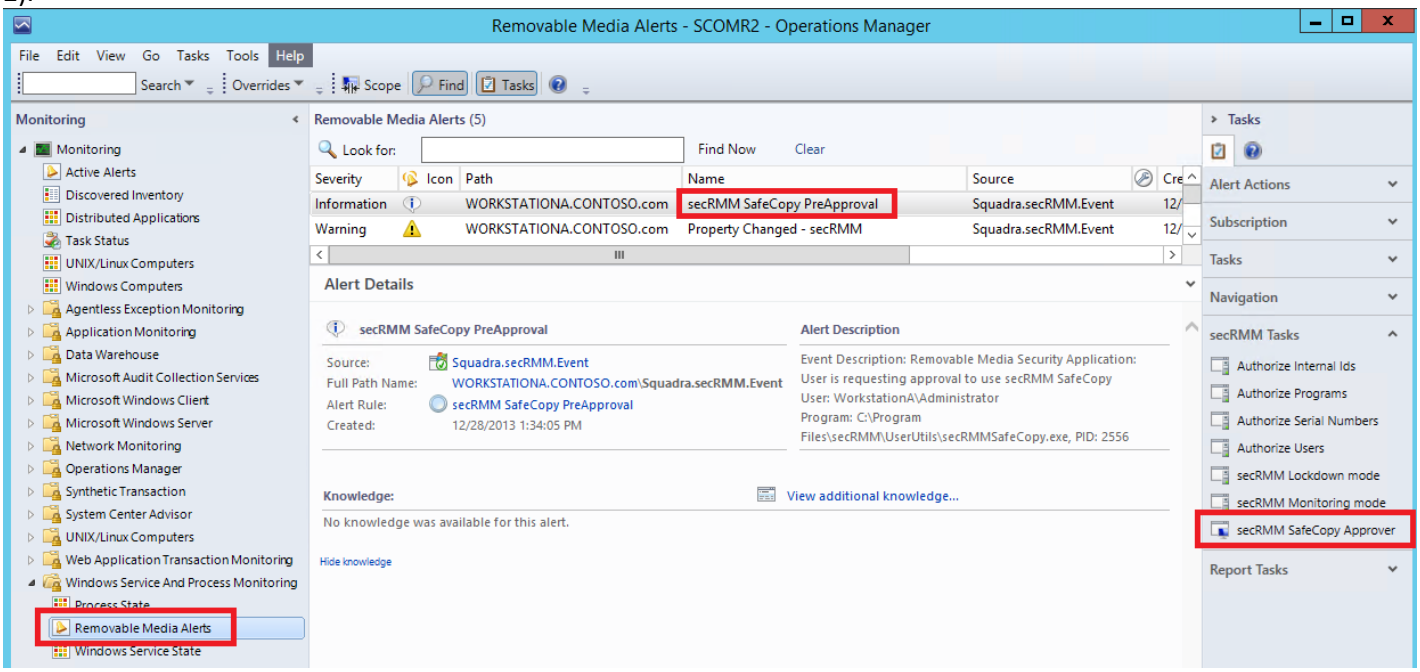
1. Click the Windows computer you want to connect to
2. Click the “Computer Management” link in the SCOM “Windows Computer Tasks”

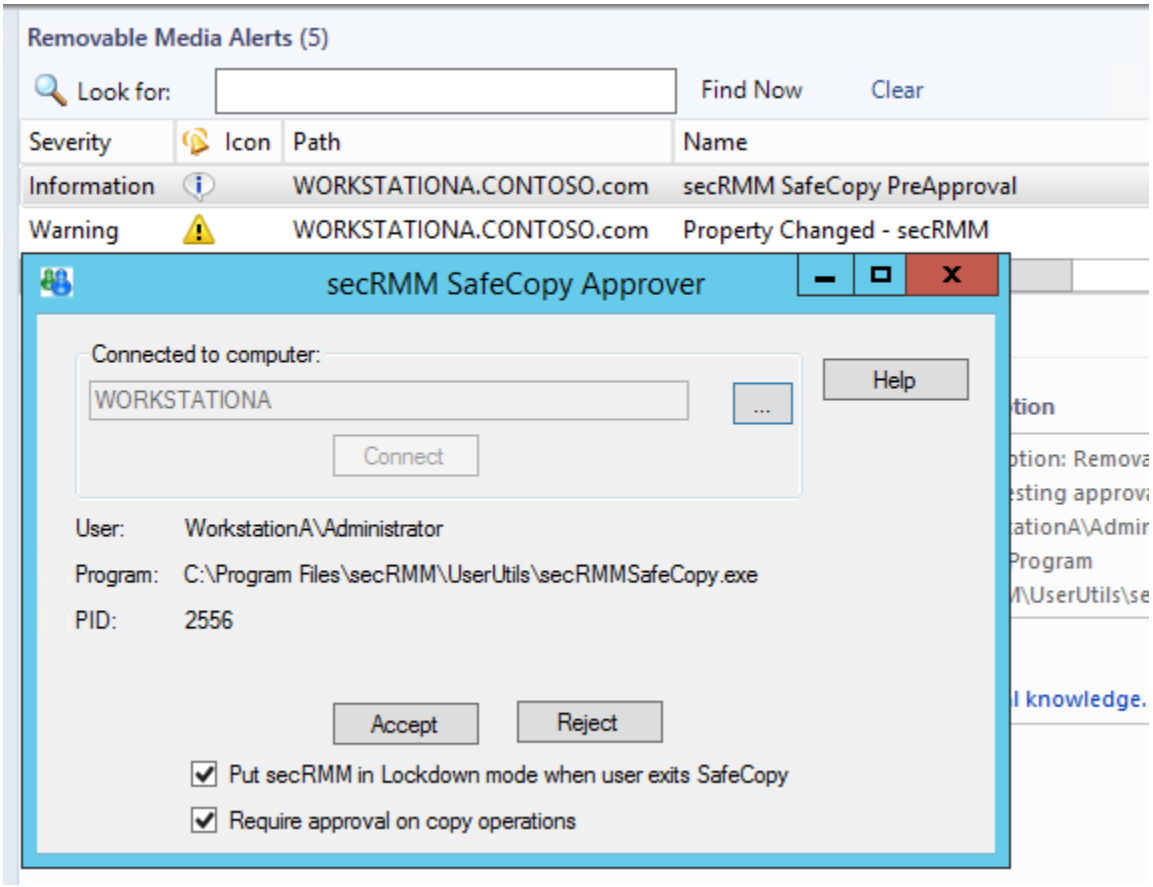




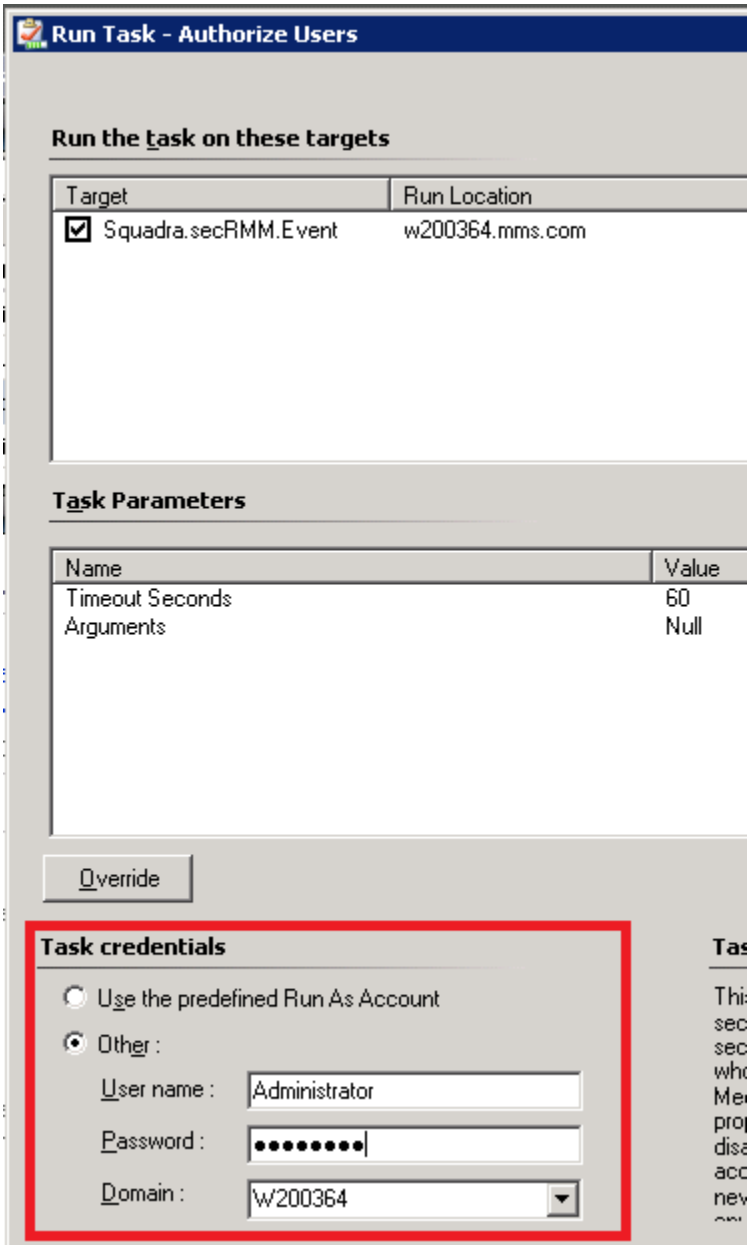
SCOM secRMM Tasks

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).

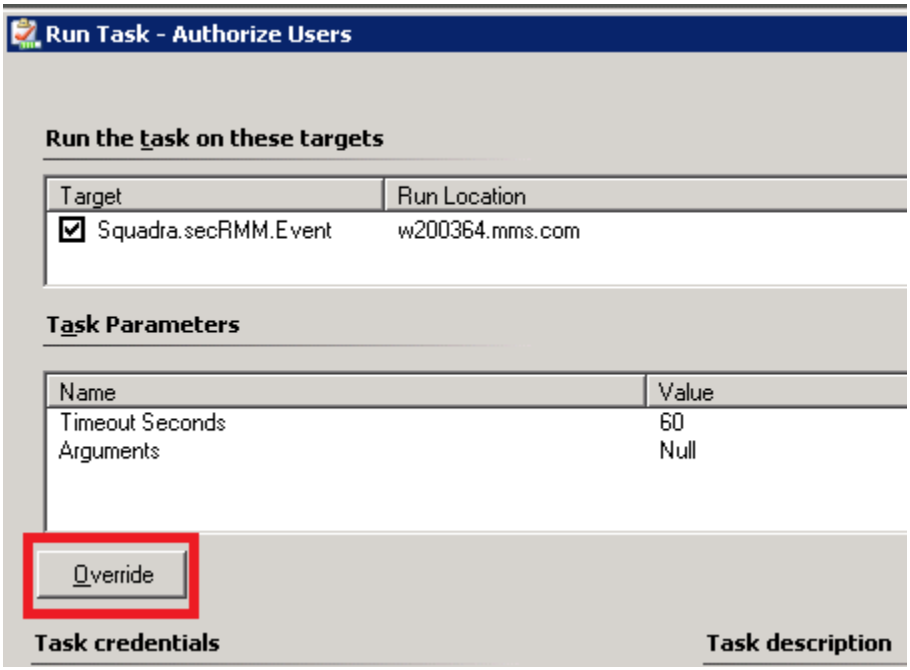


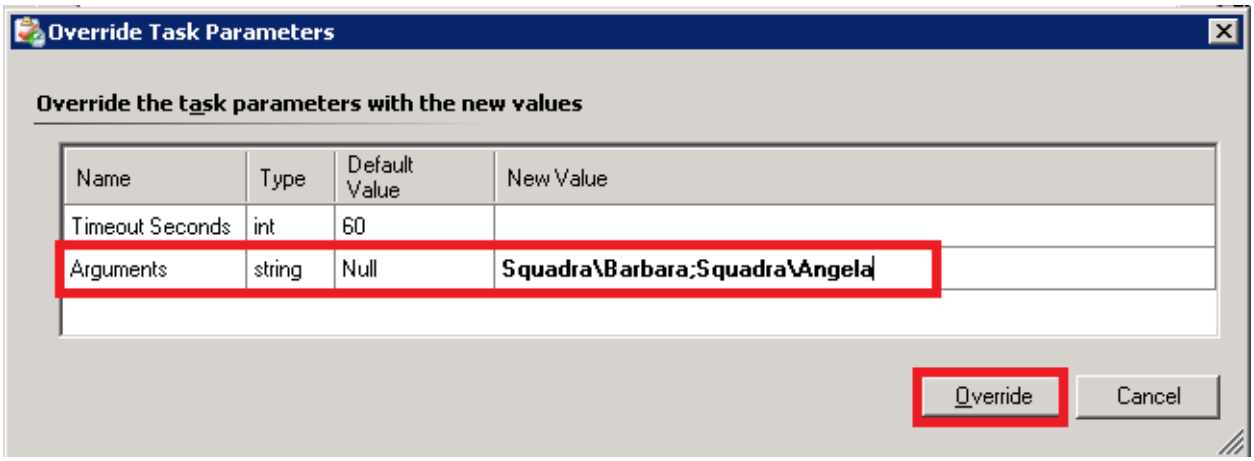


When you run the secRMM Operations Manager agent tasks, be sure that you specify an Administrator userid to run the task if the Operations Manager agent is not a member of the local Administrators group (see screenshot below). If the Operations Manager is a member of the local Administrators group on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

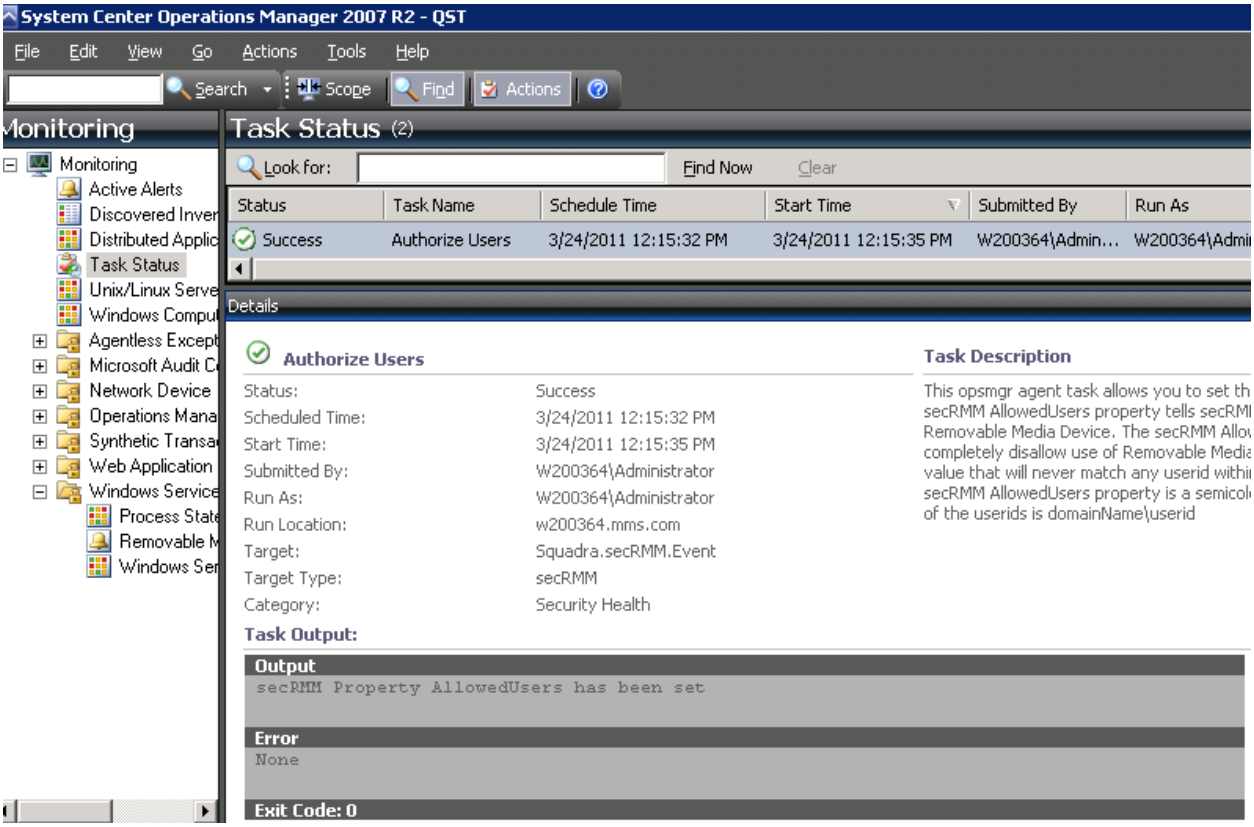


By default, the secRMM Operations Manager agent tasks are setup to clear each secRMM property (that is AllowedUsers, AllowedPrograms and AllowedSerialNumbers). If you want to use the secRMM Operations Manager agent tasks to set one of the secRMM authorization properties, you need to override the task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





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



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/