Security Removable Media Manager

SCCM 2012

Administrator Guide

Version 9.9.22.0
(January 2020)

Protect your valuable data
## Contents

### INTRODUCTION

SCCM secrMM DEPLOYMENT/INSTALLATION ............................................................... 5
SCCM secrMM CONSOLE EXTENSION ........................................................................ 5
SCCM secrMM STATUS MESSAGES .......................................................................... 6
SCCM secrMM REPORTS ......................................................................................... 7
SCCM/InTUNE CONNECTOR/secRMM INTEGRATION .................................................. 7

### INSTALLATION

SCCM secrMM CONSOLE EXTENSION ........................................................................ 8
Prerequisites ........................................................................................................... 8
SCCM features ....................................................................................................... 8
Required SCCM permissions .................................................................................... 9
Install the secrMM SCCM Console Extension .......................................................... 10
Start the SCCM Console to verify installation .......................................................... 14
Uninstalling the secrMM SCCM Console Extension ................................................... 15
SCCM secrMM STATUS MESSAGES ....................................................................... 15
Step 1 - Setting up the SCCM site server ................................................................ 15
Step 2 - Setting up the secrMM “SCCMConnection” property ................................. 20
  SCCM Security Role............................................................................................... 20
  SCCM Admins Group ........................................................................................... 23
  SCCM Security Scope .......................................................................................... 24
Step 3 – Create a SCCM Status Message query for “removable media” events ........... 24
SCCM secrMM REPORTS ......................................................................................... 30
Prerequisites ........................................................................................................... 30
Install the SCCM secrMM reports ........................................................................... 30
Install secRMM reports assembly ............................................................................ 32
Load secRMM reports into SSRS ............................................................................ 35
  Load secRMM reports into SSRS using Powershell .............................................. 35
  Load secRMM reports into SSRS manually ........................................................... 36
SCCM/InTune reports ............................................................................................. 45

### USAGE AND CONFIGURATION

SCCM secrMM CONSOLE EXTENSION ....................................................................... 46
Create a Removable Media Policy ......................................................................... 46
Deploy a Removable Media Policy ......................................................................... 50
Computer versus User deployment ........................................................................ 53
User deployment requirements ................................................................................ 53
  Windows successful logon event ......................................................................... 54
  Computer policy with SCCMConnection property defined .................................. 56
  Microsoft “.NET Framework 3.5” ....................................................................... 56
Verifying the computer policy deployment ............................................................. 58
Verifying the user policy deployment ...................................................................... 59
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation</td>
<td>60</td>
</tr>
<tr>
<td>Editing a Removable Media Policy</td>
<td>61</td>
</tr>
<tr>
<td>Deleting a Removable Media Policy</td>
<td>61</td>
</tr>
<tr>
<td>SCCM Reporting</td>
<td>61</td>
</tr>
<tr>
<td>SCCM secRMM Status Messages</td>
<td>63</td>
</tr>
<tr>
<td>Using the secRMM Excel AddIn</td>
<td>68</td>
</tr>
<tr>
<td>SCCM secRMM Reports</td>
<td>69</td>
</tr>
<tr>
<td>Browser</td>
<td>69</td>
</tr>
<tr>
<td>SCCM console</td>
<td>72</td>
</tr>
<tr>
<td>SCCM/InTune reports</td>
<td>75</td>
</tr>
<tr>
<td>STATUS MESSAGE MANAGEMENT FOR SEC RMS</td>
<td>76</td>
</tr>
<tr>
<td>STATUS MESSAGE VIEWER</td>
<td>76</td>
</tr>
<tr>
<td>VBSCRIPT</td>
<td>80</td>
</tr>
<tr>
<td>POWERSHELL</td>
<td>81</td>
</tr>
<tr>
<td>SQL</td>
<td>83</td>
</tr>
<tr>
<td>TROUBLESHOOTING</td>
<td>84</td>
</tr>
<tr>
<td>SCCM secRMM CONSOLE EXTENSION</td>
<td>84</td>
</tr>
<tr>
<td>SCCM secRMM USER POLICIES</td>
<td>85</td>
</tr>
<tr>
<td>Validation</td>
<td>85</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>85</td>
</tr>
<tr>
<td>KNOWN ISSUES</td>
<td>86</td>
</tr>
<tr>
<td>CONTACTING SQUADRA TECHNOLOGIES SUPPORT</td>
<td>86</td>
</tr>
<tr>
<td>ABOUT SQUADRA TECHNOLOGIES, LLC</td>
<td>86</td>
</tr>
</tbody>
</table>
Introduction

Security Removable Media Manager (secRMM) integrates into Microsoft System Center Configuration Manager (SCCM) 2012 by providing a SCCM console extension which provides centralized configuration, SCCM status messages and SCCM reports. secRMM can also be deployed into your domain using SCCM.

SCCM secRMM deployment/installation

The documentation for deploying/installing secRMM using SCCM is provided in a separate document called SCCM Installation Guide. You can get the SCCM Installation Guide from the Squadra Technologies web site as shown in the screen shot to the right.

http://squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx

SCCM secRMM Console Extension

The SCCM secRMM console extension builds on top of the base SCCM Compliance Settings feature. Implementing compliance settings for your corporate removable media policy rounds out the endpoint protection provided by Microsoft via:

1. Antimalware Policies
2. Windows Firewall Policies
3. BitLocker Policies (i.e. encryption technology)
4. Software updates/patching

The secRMM SCCM User Interface (UI) is identical to the secRMM UIs in the Computer Management MMC and the Active Directory Group Policy Object Editor (AD GPO).

Using one or combining the Microsoft technologies with secRMM keeps your environment safe from data theft via removable media such as USB drives/sticks, SD-Cards, Smart-Phones, Tablets, and CD/DVD. In addition to protecting your data, secRMM provides the most detailed audit trail which allows you to track every write operation to removable media.
secRMM records removable media events into an event log (named secRMM) and also into the default security event log on each computer where secRMM is installed. You can setup SCCM so that the secRMM events are displayed in the SCCM console as SCCM “status messages”. This allows you to see all the removable media events in one central location. If you have System Center Operations Manager (SCOM) installed in your environment, you can use the SCOM secRMM “Management Pack” to centralize your removable media events as well.

SCCM secRMM Status Messages

secRMM records removable media events into an event log (named secRMM) and also into the default security event log on each computer where secRMM is installed. You can setup SCCM so that the secRMM events are displayed in the SCCM console as SCCM “status messages”. This allows you to see all the removable media events in one central location. If you have System Center Operations Manager (SCOM) installed in your environment, you can use the SCOM secRMM “Management Pack” to centralize your removable media events as well.
SCCM secRMM Reports

If you setup SCCM to collect the removable media events from the secRMM event logs (i.e. SCCM status messages), you can then also load the SCCM secRMM reports into SCCM.

Please follow the steps in the next section to perform the installation of the SCCM secRMM components mentioned above.

SCCM/Intune connector/secRMM Integration
secRMM can be configured to prohibit (block) mobile devices from connecting over a USB connection if it is not enrolled in a “mobile device management” (MDM) framework. Currently, secRMM supports the Microsoft MDM named Intune. If you do have Intune in your environment, it is hosted in your organization’s Azure instance. Please contact Squadra Technologies support if you wish to use this feature.

Installation

SCCM secRMM Console Extension

If you have not already done so, please install the SCCM Console on the system where you want to run the secRMM SCCM console extension.

Prerequisites

SCCM features

The following SCCM features must be installed/enabled:

1. Client Settings->Compliance Settings must be enabled
You can verify that “Compliance Settings” are enabled on the client Windows computer(s) by going into the SCCM client program (in “Control Panel”->“System and Security”->Configuration Manager->[tab]Components):

**Required SCCM permissions**

To use the secRMM SCCM Console Extension to configure the secRMM settings, you need to have the following SCCM Security Roles assigned to your SCCM account:

1. Compliance Settings Manager
2. Endpoint Protection Manager

Note that if you are an SCCM Administrator, you will have these SCCM Security Roles assigned to your SCCM account.
Install the secRMM SCCM Console Extension

Extending the SCCM Console is an easy task. It involves copying one XML file and four dlls into the correct SCCM directory. There is an Install.cmd which will perform copying the files to the correct directories for you.

1. Download the secRMMSCCMConsoleExtension.zip file from the Squadra Technologies web site.
   a. On the Squadra Technologies Home Page, click the “System Center” logo

![System Center](image)

b. Click the “System Center Configuration Manager” link

![System Center Products](image)

   c. Click the “secRMMSCCMConsoleExtension.zip” link to download.
2. Unzip the secRMMSCCMConsoleExtension.zip file into a temporary directory on the Windows computer where you have installed the SCCM Console.
3. Close the SCCM console (if it is open).
4. Open a command window (with “Run As Administrator”).
5. In the command window, change directory (CD) into the temporary directory where you unzipped secRMMSCCMConsoleExtension.zip (from step 2 above).
6. Check to make sure that all 9 files that were unzipped are unblocked (see screen shot below). Windows blocks these files because they were downloaded from the Internet. Unfortunately, Windows does not allow you to unblock them all at once; you must go one-by-one to unblock them.
7. From the command window you opened in step 4 above, run the Install.cmd by typing Install.cmd and then hitting the enter key.

The Install.cmd logic copies the RemovableMedia.xml, secRMMSCCM2012ConsoleExtension.dll, secRMMMMCSSnapInSelectUsers.dll, secRMMMMCSSnapInSelectUsersLib.Interop.dll and secRMM10.dll into the correct SCCM directories.
The secRMM SCCM Console Extension is now available in the SCCM Console on this particular Windows Computer. If you want to use the secRMM SCCM Console on other Windows computers, you will repeat this same process on the other Windows computer(s). Note, that you do not need to have the base secRMM product installed to use the secRMM SCCM Console Extension (with one exception) although we highly recommend that you install secRMM on each Windows computer in your environment. The only time you would need to also install the secRMM product on the computer running the console extension is if you want to use the SCCMConnection property (discussed below) “Test Connection” feature. The “Test Connection” feature calls secRMM to perform the test connection to SCCM.
Start the SCCM Console to verify installation

Start the SCCM console (Microsoft.ConfigurationManagement.exe).

Once the SCCM console is open, open the “Endpoint Protection” folder (in the SCCM “Assets and Compliance” view) and verify that the “Removable Media Policies” node appears.
Uninstalling the secRMM SCCM Console Extension

If you need to uninstall the secRMM SCCM Console Extension, open a command window (with “Run As Administrator”). In the command window, change directory (CD) into the temporary directory where you unzipped secRMMSCCMConsoleExtension.zip. Be sure you first close the SCCM console before the next step. Run the Uninstall.cmd by typing Uninstall.cmd and then hitting the enter key. The Uninstall.cmd logic deletes the files that were installed from the SCCM directories. Once you restart the SCCM console on this particular Windows Computer, the “Removable Media Policies” node under the “Endpoint Protection” will be removed.

SCCM secRMM Status Messages

Installation of the SCCM secRMM status messages requires 3 steps. Step 1 is performed on the SCCM site server. Step 2 is configuring the secRMM property named SCCMConnection which you can do using the SCCM secRMM Console Extension (or Active Directory Group Policy or locally using the Computer Management MMC). Step 3 is adding a status message query in the SCCM console to see the “Removable Media Activity” events generated by secRMM.

Step 1 - Setting up the SCCM site server

1. Please take a full database backup of your SCCM database before performing the steps below since it modifies the SCCM site control file (which, since SCCM 2012, is now stored in the database instead of a file). https://msdn.microsoft.com/en-us/library/hh948978.aspx

To see the SCCM site control file contents, you can run a SQL query against your SCCM database: SELECT SiteControl FROM vSMS_SC_SiteControlXML WHERE SiteCode = 'XXX' where XXX is the 3 letter site code for your SCCM environment. Then copy the XML into a text editor (such as Visual Studio) to review your site control file (which is XML text).

2. Download the secRMMSCCMStatusMsgInstallOnServer.zip file from the Squadra Technologies web site.
a. On the Squadra Technologies Home Page, click the “System Center” logo

![System Center Logo](image)

b. Click the “System Center Configuration Manager” link

<table>
<thead>
<tr>
<th>Product</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System Center Configuration Manager (SCCM)</td>
<td></td>
</tr>
<tr>
<td>System Center Operations Manager (SCOM)</td>
<td></td>
</tr>
<tr>
<td>Azure Operations Management Suite (OMS)</td>
<td></td>
</tr>
<tr>
<td>Azure Intune</td>
<td></td>
</tr>
<tr>
<td>System Center Orchestrator</td>
<td></td>
</tr>
</tbody>
</table>

c. Click the “secRMMSCCMStatusMsgInstallOnServer.zip” link to download.

<table>
<thead>
<tr>
<th>Item</th>
<th>Download link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy/install secRMM using SCCM</td>
<td>secRMM SCCM Installation Guide (PDF)</td>
</tr>
<tr>
<td>secRMM SCCM Administrator Guide</td>
<td>secRMM SCCM Administrator Guide (PDF)</td>
</tr>
<tr>
<td>secRMM SCCM Console Extension download</td>
<td>secRMMSCCMConsoleExtension.zip</td>
</tr>
<tr>
<td>secRMM SCCM Status Messages download</td>
<td>secRMMSCCMStatusMsgInstallOnServer.zip</td>
</tr>
<tr>
<td>secRMM SCCM Reports download</td>
<td>secRMMSCCMReports.zip</td>
</tr>
<tr>
<td>SecRMM SCCM/Intune Reports download</td>
<td>secRMMSCCMIntuneReports.zip</td>
</tr>
<tr>
<td>secRMM SCCM Status Message Cleanup Utility</td>
<td>secRMMSCCMDeleleByMessageText.vbs</td>
</tr>
<tr>
<td>secRMM Intune Access Control Setup Guide</td>
<td>secRMMIntuneAccessControlSetupGuide.pdf (PDF)</td>
</tr>
</tbody>
</table>

3. Unzip the secRMMSCCMStatusMsgInstallOnServer.zip file into a temporary directory on the SCCM site server.

4. Open a command window (with “Run As Administrator”).

5. In the command window, change directory (CD) into the temporary directory where you unzipped secRMMSCCMStatusMsgInstallOnServer.zip.

6. Check to make sure that all 7 files (there is one dll in each subfolder) that were unzipped are unblocked (see screen shot below). Windows blocks these files because they were downloaded from the Internet.
7. Run the Install.cmd by typing Install.cmd and then hitting the enter key. The Install.cmd calls the program AddSecRMMToSCCMStatusMessages.exe which updates the SCCM site control file and adds the secRMMSCCMMsgs.dll into the SCCM status messages directories. This program will prompt you for your SCCM 3 letter site code\(^1\). When it prompts you for the server, make sure to put a period (“.” – the period indicates you are running on the site server) and hit enter.

---

\(^1\) If you do not know the SCCM 3 letter site code, you can open the SCCM console, click Administration (in the lower left hand corner), in the tree view, go to Overview->Site Configuration->“Servers and Site
8. The output from program AddSecRMMToSCCMStatusMessages.exe should look like:

System Roles”. Now, on the right hand side of the console, you will see a list of servers. There is a column labeled “Site Code”.
9. You should now restart the SMS_EXECUTIVE service.
10. To verify that SCCM is now using the secRMM messages dll, you can check the smsexec.log file and search for the text saying:

*Registered this process as a source of "secRMM" events.*

![Log File Screenshot](image)

11. Note that if you install the SCCM console on a remote computer (i.e. not the site server), you will still need to copy the dll named secRMMSCCMMsgs.dll from the Win32 directory to C:\Program Files(x86)\Microsoft Configuration Manager\AdminConsole\bin\i386\00000409. If you do not perform this step and try to open the SCCM “Status Message Viewer” against the “Removable Media Activity” query (described in Step 3 below), the “Status Message Viewer” will crash. As a convenience, if you install the SCCM secRMM console extension on the remote computer, the secRMM console extension installation will copy the secRMMSCCMMsgs.dll file for you.

**Step 2 - Setting up the secRMM “SCCMConnection” property**

secRMM needs to be able to connect to SCCM with credentials from a valid SCCM user account. You need an Active Directory userid for this step. There are 2 things to setup for this userid to allow the secRMM to SCCM connection:

1. The userid needs a “SCCM Security Role”
2. The userid needs to be in the local “SMS Admins” Group on the SCCM site server computer

**SCCM Security Role**

The SCCM user account has to belong to at least one of the following SCCM “Security Roles”:

1. Full Administrator
2. Asset Manager
3. Infrastructure Administrator
4. Operations Administrator

These are the SCCM “Security Roles” that are allowed to add and delete status messages.

If you do not use the “Full Administrator” role and you plan on using secRMM “User Configurations”, then you must also add the “Compliance Settings Manager” SCCM “Security Role”.

So, as an example, in the two screen shots below, there is a userid named CONTOSO\secRMMSCCMConnection. This userid has the security roles: “Asset Manager” and...
“Compliance Settings Manager”. The “Asset Manager” will let secRMM create SCCM “Status Messages” and the “Compliance Settings Manager” will let secRMM create SCCM “User Collection” Policies.
SCCM Admins Group

The user you use must also be a member of the “SMS Admins” Group. This group has local and remote access to the WMI SMS Provider on the SCCM primary site server. Microsoft has a TechNet article that tells you how to verify WMI permissions to the SMS Provider at https://technet.microsoft.com/en-us/library/bb932151.aspx. You can add a user to the “SMS Admins” Group using the “Computer Management” MMC on the SCCM primary site server as shown in the screen shot below.
SCCM Security Scope

Within the SCCM console, verify that the userid has the proper associated SCCM security scope. We have had one customer who needed to make sure that the userid belonged to the “Default” security scope or else if they used the SCCM console remotely, they were unable to open the “Removable Media Policies” node in the SCCM tree view. The console was crashing when they had specified the wrong SCCM security scope. We believe this is caused by a permissions issue when remotely connecting to the SCCM WMI Provider on the SCCM site server.

Step 3 – Create a SCCM Status Message query for “removable media” events

Within the SCCM console, under the Monitoring->“System Status” node, you can create a “status message” query for the secRMM event data. For naming consistency, we recommend you name the query “Removable Media Activity”.

Component = secRMM
Create Status Message Query Wizard

General

Name: Removable Media Activity

Comment: Event data generated by secRMM

Import Query Statement...

Edit Query Statement

Query Statement Properties

Specify the attributes to search for and how they will be displayed when the query is run.

Find objects of type: Status Messages

Omit duplicate rows (select distinct)

Results:

<table>
<thead>
<tr>
<th>Class</th>
<th>Attribute</th>
<th>Sort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Messages</td>
<td>&lt;All attributes&gt;</td>
<td>&lt;Unsort...</td>
</tr>
<tr>
<td>Status Message Strings</td>
<td>&lt;All attributes&gt;</td>
<td>&lt;Unsort...</td>
</tr>
<tr>
<td>Status Message Properties</td>
<td>&lt;All attributes&gt;</td>
<td>&lt;Unsort...</td>
</tr>
</tbody>
</table>

Show Query Language
where SMS_StatusMessage.Component = 'secRMM'
Create Status Message Query Wizard

Summary

Create a new status message query.

Details:

Create a new status message query.
- Name: Removable Media Activity

To change these settings, click Previous. To apply the settings, click Next.
SCCM secRMM Reports

Prerequisites

If you are not already using reporting in your SCCM environment, you will need to set up the environment per Microsoft’s instructions at: https://technet.microsoft.com/en-us/gg712698.aspx

Install the SCCM secRMM reports

1. Download the secRMMSCCMReports.zip file from the Squadra Technologies web site.
   a. On the Squadra Technologies Home Page, click the “System Center” logo

   ![System Center Logo]

   b. Click the “System Center Configuration Manager” link

   ![System Center Configuration Manager Link]
c. Click the “secRMMSCCMReports.zip” link to download.

2. Unzip the secRMMSCCMReports.zip file into a temporary directory on the Windows computer where you have installed the SCCM Report Server. SCCM uses SQL Server Reporting Services (SSRS) as its reporting engine. The SSRS database may or may not be on the same computer as the SCCM site server. You can find out where the SSRS for SCCM is installed within the SCCM console. Go into the Monitoring view (lower left hand corner of the console), then click the Reporting folder. Now, on the right-hand side of the screen, at the bottom, you will see the URL for the Report Manager. This is shown in the screen shot below.
3. Open a command window (with “Run As Administrator”).

**Install secRMM reports assembly**

1. In the command window, change directory (CD) into the temporary directory where you unzipped secRMMSCCMReports.zip. Now change directory (CD) into the Assembly sub-directory.

2. Check to make sure that all 6 files that were unzipped in the Assembly sub-directory (see screenshot above) are unblocked (see screenshot below). Windows blocks these files because they were downloaded from the Internet.
3. In the Assembly sub-directory, edit the file named InstallAssemblyForSCCM.cmd with a text editor (notepad for example). On line 6, change the XXX to be your 3 letter site code. Save the file.
4. Now (run the script named) type InstallAssemblyForSCCM.cmd and hit the enter key.
5. The output of executing the script is a file named InstallSCCM_Output.rpt (see screenshot above). This file should look like:

![Image of InstallSCCM_Output.rpt]

This assembly that loaded into the SCCM database allows the reports to parse the secRMM event data.

**Load secRMM reports into 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).

![Image of ImportReports.cmd and ImportReports.ps1]

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 SCCM report server, open a browser and go to URL: http://localhost/reports

2. Click the “ConfigMgr_XXX” folder (where XXX is your 3 letter site code). Within the ConfigMgr_XXX folder, click the “New Folder” link.

3. Create a folder for the “Removable Media” reports. You are free to name this folder whatever makes most sense for your environment.
4. Now click the folder you just created to go into it.
5. Click the “Upload file”
6. Click the “Browse” button

7. Go to the sub-directory named Reports\SCCM_DB (in our example, we used C:|\temp\secRMMSCCMReports\Reports\SCCM_DB)
8. Select the report file (i.e file extension of .rdl) and click the OK button.

9. Repeat steps 14-16 for each file in the Reports\SCCM_DB sub-directory (there are 5 files).
10. Next, we need to modify the “Data Sources” of each report to be the “Data Sources” for your SCCM database. To do this, move your mouse to the right of the report so that you see a yellow box with an arrow pointing down (see below). Click the drop down arrow and select “Manage”.
11. Select “Data Sources”
12. A warning shows on the page stating “The shared data source reference is no longer valid”. Click the “Browse” button to the left of this warning.

13. Under the Home button, you will see your SCCM database (named ConfigMgr_XXX where XXX is your 3 letter site code). Click the plus sign (+) to the left of your SCCM database so it expands.
14. Under the SCCM database folder will be a long list of subfolders. At the very bottom, you will see an icon of a yellow cylinder (see below). It will likely not have the same letters and numbers to the right but this is the “Data Source” for your SCCM database.
15. Click the “Data Source” so it is selected and then click the OK button.

16. Click the Apply button. Now the report will use the SCCM database to get data.
17. Repeat steps 18-24 for each report.
18. Run each report to ensure no errors occur. If you get an error about permissions, please run the following sql commands from either “SQL Management Studio” or using the command line sqlcmd utility. You need to run these commands against the SCCM database (i.e. CM_xxx where xxx is your 3 character site code).

```
GRANT SELECT ON [dbo].[secRMMSQLTableValuedFunction] TO [smsschm_users]
GRANT EXECUTE ON [dbo].[CompareUserLists] TO [smsschm_users]
GRANT SELECT ON [dbo].[vStatusMessageInsStrs] TO [smsschm_users]
GRANT SELECT ON [dbo].[vStatusMessages] TO [smsschm_users]
```

**SCCM/InTune reports**

The SCCM/Intune secRMM reports are installed the same way as the base SCCM reports (detailed in the
instructions above). If you have Intune configured in your SCCM environment, you should consider also loading the SCCM/Intune secRMM reports. The zip file containing the reports is on the Squadra Technologies web site and is named secRMMSSCCMInTuneReports.zip. There are 2 reports to load into your environment. Before you load these reports, you must make one change for your environment. Edit the file named “Mobile device USB File Write Activity.rdl” using Notepad. This file is in the Reports\SCCM_DB subfolder (created when you unzipped secRMMSSCCMInTuneReports.zip). Go to line (ctrl-g when “word wrap” is off) 1281 (you can also do a find for XXX to get to line 1281). On line 1281, change the XXX to your 3 character SCCM site code.

Usage and configuration

SCCM secRMM Console Extension

The SCCM secRMM Console Extension lets you centrally configure and deploy the secRMM rules/policies for the computers and users in your domain. This feature utilizes the base SCCM “Compliance Settings” component. SCCM “Compliance Settings” give you several features:

1. Setting the secRMM rule(s) on each computer or user within your domain
2. For computer configurations, a recurring check is made of the current secRMM rule values on each computer within your domain based on the SCCM deployment schedule. For user configurations, at user logon time, a check of the current secRMM rules for the user logging into the Windows computer. For both, the following operations are performed:
   a. Reporting if a value is not in compliance
   b. Resetting the value if it is not in compliance
3. Out of the box SCCM compliance reports

The subsections below describe how to use the SCCM secRMM Console Extension.

Create a Removable Media Policy

To create a “Removable Media Policy”, you can right mouse click on either the “Removable Media Policies” node in the tree-view, right mouse click in the white space in the details view or use the SCCM ribbon bar. For the node in the tree-view, make sure you first left-click the node so the right side windows says “Removable Media Policies” before you right-mouse click it.
Clicking the “Create Removable Media Policy” function will open a window that lets you specify the secRMM property values. For details on each secRMM property, you should review the secRMM Administrators Guide. At the very top of the “Removable Media Policy” window, please specify a name, an optional description for the “Removable Media Policy” and select whether this policy will be for computers or users. Then, provide the values for one or more secRMM properties. To edit a property, double click the row and another windows will open allowing you to specify a value. At a minimum, you should always turn on the “FailWriteIfSourceFileUnknown” secRMM property. This sets secRMM in “monitoring mode”. You need to specify at least one secRMM property before you can save the policy.

Below are two screen shots, the first one is a Computer policy and the second is a User policy. You must define one Computer policy and at a minimum, specify the SCCMConnection property. The SCCM logon credentials specified in the SCCMConnection property allows secRMM to send the secRMM event data to SCCM. Once the secRMM events data is sent to SCCM, you can view this secRMM event data using SCCM Status Messages and SCCM secRMM reports.
### Removable Media Policy Editor

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllowBitLockerOnly</td>
<td></td>
</tr>
<tr>
<td>AllowedDirectories</td>
<td></td>
</tr>
<tr>
<td>AllowedFileExtensions</td>
<td></td>
</tr>
<tr>
<td>AllowedInternalIds</td>
<td></td>
</tr>
<tr>
<td>AllowedPrograms</td>
<td></td>
</tr>
<tr>
<td>AllowedSerialNumbers</td>
<td></td>
</tr>
<tr>
<td>AllowedUsers</td>
<td></td>
</tr>
<tr>
<td>BlockCDROMAndDVDWrite</td>
<td></td>
</tr>
<tr>
<td>BlockOfficeMacrosOnDevice</td>
<td></td>
</tr>
<tr>
<td>BlockProgramsOnDevice</td>
<td></td>
</tr>
<tr>
<td>EnableRMS</td>
<td></td>
</tr>
<tr>
<td>FailWriteIfSourceFileUnknown</td>
<td>on</td>
</tr>
<tr>
<td>HashAlgorithm</td>
<td></td>
</tr>
<tr>
<td>LogSecurityEventsAsFailures</td>
<td>on</td>
</tr>
<tr>
<td>LogWriteDetails</td>
<td></td>
</tr>
<tr>
<td>MonitorCDROMAndDVD</td>
<td>on</td>
</tr>
<tr>
<td>MonitorFloppyDrive</td>
<td></td>
</tr>
<tr>
<td>PreApproveSafeCopy</td>
<td></td>
</tr>
<tr>
<td>RequireSmartPhoneLogin</td>
<td></td>
</tr>
<tr>
<td>ScanDevice</td>
<td></td>
</tr>
<tr>
<td>SCCMConnection</td>
<td>SCCMR2</td>
</tr>
<tr>
<td>SendEmail</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td>Syslog</td>
<td></td>
</tr>
</tbody>
</table>

Please remember that if you modify a policy, you must redeploy it.
NOTE: It is highly recommended that, as a minimum, you always turn on: FailWriteIfSourceFileUnknown.

Once you have specified one or more secRMM properties, click the OK button to save your changes. You will now see the “Removable Media Policy” in the list.
Deploy a Removable Media Policy

Since the secRMM Console Extension is based on the “SCCM Compliance Settings”, you will deploy the “Removable Media Policy” just as you would for any other SCCM Compliance Setting.

In the SCCM tree view, expand the “Compliance Settings” folder and then the “Configuration Baselines” folder. You will see a folder named “Removable Media Policies”. If you do not see this folder, click Refresh (F5). It may take several Refreshes depending on how busy SCCM is. If you still cannot see the Compliance Settings item, sometimes, clicking on the parent folder (i.e. the folder named “Compliance Settings”) and hitting refresh on that folder will force the subfolders to refresh. Under the “Removable Media Policies” folder, you will see a folder with the same name as the “Removable Media Policy”. Click that folder and the “Configuration Baseline” will appear in the details pane. Right mouse click on the “Configuration Baseline” and select “Deploy”.
If you are familiar with the deployment options, you may set the values to best suit your environment. An important value for you to consider on the deployment dialog is the “Run every” value. This is how often SCCM will check that the policy is compliant.

Note that for Computer configurations, you MUST check the “Remediate noncompliant rules when supported” and the “Allow remediation outside the maintenance window” checkboxes. Failure to check these two checkboxes will result in the policy not being applied on the computers you are deploying the policy to.

Below is a valid recommendation.
Before closing the “Deploy Configuration Baselines” window, you must select a collection to deploy to. Click the “Browse” button (outlined in the blue box above).

For computer policies, select “Device Collections” and then select a collection from the available device collections defined in your environment.

For user policies, please select a collection from the available user collections.
The “Removable Media Policy” is now deployed.

**Computer versus User deployment**

The “computer deployment” will run on a scheduled task where the time interval will be what you specified in the deployment dialog. SCCM sends the “computer deployment” secRMM policy down to the SCCM clients during a “Machine Policy Retrieval & Evaluation Cycle”. You can force a “Machine Policy Retrieval & Evaluation Cycle” to happen on a client SCCM computer using the SCCM client GUI, under the Actions tab. This is shown in the “Verifying the computer policy deployment” section below.

A “user deployment” will run whenever the user logs into a Windows computer with secRMM installed on it. “User deployments” take effect immediately since it is triggered by the user logging into a computer.

**User deployment requirements**

There are four requirements to making a user deployment work:

1. The Windows computer where the user logs in must be generating “successful logon events” (event id 4624) into the Windows security event log
2. A secRMM “computer policy” with the SCCMConnection property defined.
3. The secRMM version must be at 7.0.6.0 or better
4. The Microsoft .NET Framework version 3.5

The details of these requirements are explained below.
**Windows successful logon event**

To make a user deployment run whenever the user logs on to a Windows computer, the Windows computer must be generating a “successful logon event” (event id 4624) in the security event log. This event triggers the SCCM user policy to be checked on the computer for the user. Microsoft documentation for event id 4624 is located at [https://technet.microsoft.com/en-us/library/dn319080.aspx](https://technet.microsoft.com/en-us/library/dn319080.aspx). You can enable auditing (i.e. generating) successful logon events using either a SCCM Task Sequence or Active Directory Group Policy Object (AD GPO). You should first check in your environment to see if this event is already being generated. It is typically a common event to generate so you may not need to do anything if the event is already being generated. The setting is in **Computer Configuration/Windows Settings/Security Settings/Advanced Audit Policy Configuration/Audit Policies/“Logon/Logoff”** and is called **Audit Logon**. At a minimum, you must set the "Success" value.
Details about event id 4624 are at: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings.
**Computer policy with SCCMConnection property defined**

Each computer that will support user policies will need a secRMM “computer policy” defined on the computer as well. There can only be one secRMM “computer policy” on a computer. The computer policy should be very restrictive since it is the default policy that is used if the user is not assigned to a “user policy”. For example, the “computer policy” might put secRMM in lockdown mode (meaning no file copies to removable storage is allowed). Regardless of the authorization or lockdown policy you choose for the “computer policy”, you will need to specify the SCCMConnection property. The SCCM logon credentials specified in the SCCMConnection property will allow the user policy to retrieve the policy from SCCM.

**Microsoft “.NET Framework 3.5”**

For user policies, your endpoint computers will need to have the Microsoft “.NET Framework 3.5” installed. On pre-Windows 10 computers, it is likely to already be installed. The screenshots below show how to install the Microsoft “.NET Framework 3.5”. If do not plan on using user policies, you can skip this prerequisite.
Verifying the computer policy deployment

Go to one of the Windows computers that is in the collection that you selected in the deployment. Open the SCCM client program (in “Control Panel”->“System and Security”).
Click the Actions tab. In the list of Actions, click the “Machine Policy Retrieval & Evaluation Cycle”. Click the “Run Now” button. This will download the “Removable Media Policy” to the computer. Note that depending on the size of your environment, this process could take a while to complete.

To verify that the “Removable Media Policy” has been downloaded, click the Configuration tab. You will see the “Removable Media Policy” with the name you assigned it when it has been downloaded. Notice in the left hand screen shot below, the “Last Evaluation” column has a value of N/A and the “Compliance State” column has a value of Unknown. This means the “Removable Media Policy” has not run yet. To run the “Removable Media Policy”, click the Evaluate button at the bottom of the window. Once the “Removable Media Policy” has been evaluated, the “Last Evaluation” column and the “Compliance State” column will have valid values as shown in the right hand screen shot below.

Please note that you do not need to click the “Evaluate” button on every computer you deploy to (that would be unrealistic). Clicking it on your test computers just makes the evaluation run “right now”. The SCCM client programmatically performs what the “Evaluate” button does at a repeating scheduled interval. This interval value is specified when you deploy the “Removable Media Policy”.

Once the “Removable Media Policy” has been evaluated, you can view a report by clicking on the “View Report” button at the bottom of the window.

Verifying the user policy deployment

You cannot use the verification process for the user policies as we did for the computer policies in the section above. This is because SCCM does not really push down the user policy. secRMM has to pull it from SCCM when the user logs in. The best way to verify the user policy is to use the secRMM event log on the computer where the user logged in. If the policy was being defined for the first time or the policy needed to be “remediated”, you will see an event for each secRMM property that was modified as in the screen shot below:
If you study the data in the red box carefully, you will see that the secRMM property named AllowedDirectories was set by the user policy named “User Policy 1”, Revision 1 for the user CONTOSO\Angela.

**Remediation**

For computer policies, when you deploy the “Removable Media Policy”, you must select to correct any property value that is not the value you specify in the “Removable Media Policy”. This is called remediation. If remediation does occur, the SCCM report will show this as compliant because the value was changed back to the compliant value. To see which properties were changed, you can look in the secRMM event log. If remediation does occur, you will see an event in the secRMM event log. The event contains the details of the property being changed. The event is shown below:

Below is the text taken from the screen shot above. Notice on the last line, it indicates that the value was changed back by SCCM remediation.
Removable Media Security Authorization:
Administrator: NT AUTHORITY\SYSTEM, SID: S-1-5-18
Action: secRMM Property created
Property name: AllowedDirectories
Property value: C:\Users\<UserId>;<d:\temp
Property set for: CONTOSO\angela, SID: S-1-5-21-194330278-343332919-2867172138-1606
Status: Completed
Additional Event Info: C:\Windows\System32\cscript.exe" //NoLogo //B C:\Windows\Temp\rad30BE6.js

SCCM Compliance Setting Remediation for AllowedDirectories. Type: User, Name: User Policy 1,
Revision: 1, CONTOSO\Angela, S-1-5-21-194330278-343332919-2867172138-1606

Editing a Removable Media Policy

You can edit an existing “Removable Media Policy” by using either the secRMM Console Extension or by using the base Microsoft SCCM Compliance Settings windows. If you edit the “Removable Media Policy” by using either the secRMM Console Extension, it will retain the existing values in the Configuration Item Baseline (i.e. the values you specified for the deployment part).

If you do edit a Removable Media Policy, you must re-deploy it. Every time you modify a “Removable Media Policy”, the SCCM Revision value gets incremented by 1. You should set the SCCM console to show the Revision number column on the “Removable Media Policies”. The SCCM Revision number is also visible in the SCCM client GUI on the Configurations tab. This is a good way to see that the modified “Removable Media Policy” has been pushed down to the client.

We are looking into how to avoid requiring a re-deployment for a future release of the SCCM secRMM Console Extension.

Deleting a Removable Media Policy

You can delete an existing “Removable Media Policy” by using either the secRMM Console Extension or by using the base Microsoft SCCM Compliance Settings windows. If you delete the “Removable Media Policy” by using either the secRMM Console Extension, it will delete:

1. Configuration items
2. Configuration item folder for the “Removable Media Policy”
3. Configuration baseline
4. Configuration baseline folder for the “Removable Media Policy”

SCCM Reporting

SCCM has several “Compliance and Settings Management” reports. The reports are under Monitoring->Reporting->Reports. These reports will include the data from the Removable Media Policies.
In addition, you can view a report directly from a SCCM client computer by using the “Configuration Manager” User Interface located in “Control Panel” -> “System and Security” (on the client computer).
SCCM secRMM Status Messages

The SCCM Status Messages for secRMM data are dependent on the SCCM credentials provided in the SCCMConnection property of secRMM. You specify the secRMMConnection from within one of the secRMM User Interface dialogs.

The dialogs are:

1. The secRMM SCCM Console Extension
2. The secRMM Active Directory Group Policy
3. The secRMM “Computer Management” MMC
Since you are reading this document, it is most likely that you will use the secRMM SCCM console extension to set the SCCMConnection property.

You have the ability to perform a “Test Connection” operation. You should try to perform this test on a computer that is not the SCCM site server if possible. The reason to perform the test on a computer that is not the SCCM site server is because when performed on the SCCM site server, the userid/password test does not get performed (because you are already on the SCCM site server).
Ultimately, the secRMM SCCMConnection property gets treated like all the other secRMM properties in that it gets deployed down to the computers running secRMM. Once the SCCMConnection property is set on the computers, they will start sending status messages (i.e. the secRMM event data) to the SCCM site server.
Using the secRMM Excel AddIn

The secRMM Console Extension also provides a call to the secRMM Excel AddIn. The secRMM Excel AddIn can load the SCCM status messages. This allows you to view the SCCM status messages from within Excel. Please refer to the Excel AddIn Administrator Guide to install the secRMM Excel AddIn. Note that the Excel AddIn will be installed on the same computer where the SCCM Administrator Console is installed. The Excel AddIn uses the secRMM SCCMConnection property to communicate with SCCM.

If you try to use the secRMM Excel AddIn from with the SCCM console and you get an “Access Denied”, simply reopen the SCCM console using “Run As Administrator”.

![Image of secRMM Excel AddIn interface]
SCCM secRMM Reports

You can run the SCCM “Removable Media” (i.e. secRMM) reports from either a browser or directly within the SCCM console. The Microsoft reporting engine (SQL Server Reporting Services, i.e. SSRS) has many powerful features including scheduling reports to be delivered to your email inbox on a recurring schedule (in various formats, including excel and pdf). You should follow the Microsoft documentation on SSRS to gain the full benefits of the reporting component of SCCM.

Browser

The SCCM SSRS website has a default URL of http://ComputerName/reports. This may vary in your environment. Once you are at the home page, click the link referencing your SCCM database.
Scroll down until you see the “Removable Media” subfolder. Click the “Removable Media” subfolder.

Select one of the “Removable Media” reports to run.
In this example, we will run an “Authorization Failure” report:

The above report shows there is currently only one authorization failure within the domain.

In addition to the reports provided by the secRMM product, you can run the Microsoft SCCM “Compliance and Settings Management” reports as well.
SCCM console

The SCCM reports are located within the console under Monitoring->Reports. There are many reports provided by Microsoft. The reports are listed in alphabetical order so scroll down to “R”. Under “R”, you will see reports starting with “Removable Media”.

Select one of the “Removable Media” reports to run.
In this example, we will run a “Write Events” (i.e. files written from the domain to a removable media device) report. Notice that the report dialog needs to specify a “User Name”. Click the “Values...” link and select a value.
To run the report, click the “View Report” button.
Here we can see a report that lists all the removable media write activity for the specific user. There are too many columns in this report to show you all the valuable data within this report in a single screen shot so please run the reports in your environment so you can see that value of the secRMM data!

![Removable Media Write Events]

**SCCM/InTune reports**

To associate the Intune mobile device definitions to the secRMM event data, you must run the LinkMobileDevices.exe utility that is in the Utility subfolder (created when you unzipped secRMMSCCMInTuneReports.zip). This program will list the mobile devices being managed by SCCM/InTune. For each mobile device, you will need to provide the mobile devices serial number as secRMM knows it. Unfortunately, InTune does not seem to be capable of recording the true/firmware serial number of the mobile devices (we hope this will be fixed in later InTune releases). For now, you will need to generated a secRMM ONLINE event for the mobile device by connecting the device to a Windows computer running secRMM with a USB cable. Once Windows mounts the mobile device, you will see an online event in the secRMM event log. Plug the serial number from secRMM into the corresponding row in the LinkMobileDevices.exe utility.
Status Message Management for secRMM

The secRMM event data is forwarded from the endpoint computers to the SCCM site server and into the SCCM database. SCCM terms this data as “Status Messages”. “SCCM Status Messages” are used extensively by Microsoft to record events that are happening within SCCM. This is the same mechanism that secRMM uses (i.e. the secRMM event data is stored within the SCCM SQL tables/views just the same as native SCCM Status Messages). You should periodically export (and then delete from the SCCM database) the “secRMM SCCM Status Messages” to an external file which can then be archived. This strategy allows you to keep the security event data generated by secRMM for historical and post-analysis. It also keeps the SCCM database from growing without bound and allows the secRMM reports to load quickly. You have options on how you can export the “secRMM SCCM Status Messages” from the SCCM database. The options are:

1. Status Message Viewer
2. VBScript
3. PowerShell
4. SQL

These options are outlined below.

You should also read the “secRMM Administrators Guide”, section titled “Managing the secRMM event log”. This section discusses other options for archiving secRMM event data. In summary, the section describes using the secRMM event log to archive the data versus using SCCM. If you chose that archiving strategy, then in SCCM, you can simply delete the “secRMM SCCM Status Messages” periodically. You could also utilize secRMMCentral. secRMMCentral uses Microsoft Event Forwarding technology to forward the secRMM event data from the endpoint computers to a central event log (named secRMMCentral). From the secRMMCentral event log, you can have a scheduled task import the secRMMCentral event log into a standalone SQL server database. From the standalone SQL server database, you can run secRMM predefined reports in addition to using SQL backups for archiving.

### Status Message Viewer

<table>
<thead>
<tr>
<th>Netbios Name</th>
<th>secRMM Serial Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>tony_Android_12/1/2016_7:53 PM</td>
<td>41001e499741a000</td>
</tr>
<tr>
<td>tony_WindowsPhone_11/29/2016_11:42 PM</td>
<td>00000011E5DE51D70000000000000000</td>
</tr>
<tr>
<td>BARBARA's iPad</td>
<td>ed7199286361478d0ba764ab9561533c51ac</td>
</tr>
</tbody>
</table>
You can use the “SCCM Status Message Viewer” User Interface program to export and delete the secRMM status messages. You invoke the “SCCM Status Message Viewer” from the SCCM console “Monitoring mode” of SCCM as shown below.
### secRMM SCCM Compliance Settings Administrator Guide

![Excel screenshot showing the Text Import Wizard]

The Text Import Wizard has determined that your data is Delimited.

- **Original data type**
  - Choose the file type that best describes your data:
    - Delimited: Characters such as commas or tabs separate each field.
    - Fixed width: Fields are aligned in columns with spaces between each field.

- **Start import at row**: 1
- **File origin**: 63301: Unicode (UTF-8)
- **My data has headers.**

#### Preview of file: `secRMMSCCM_09262017.txt`

```
1. Severity, Date / Time, System, Message ID, Description
```

<table>
<thead>
<tr>
<th>Severity</th>
<th>Date / Time</th>
<th>System</th>
<th>Message ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>08/22/2017 14:30</td>
<td>secRMM</td>
<td>400</td>
<td>Removable Media Security Audit: Drive E:; Volume: \Device\HarddiskVolume9, Description: Removable media detected in E:.</td>
</tr>
<tr>
<td>Information</td>
<td>08/22/2017 14:30</td>
<td>secRMM</td>
<td>300</td>
<td>secRMM: Device E: is ONLINE in Virtual Machine host AZUREVM2 on Microsoft Hyper-V.</td>
</tr>
<tr>
<td>Information</td>
<td>08/22/2017 14:30</td>
<td>secRMM</td>
<td>403</td>
<td>Removable Media Security Audit: Drive E:; Volume: \Device\HarddiskVolume9, Description: Drive E: is offline in Virtual Machine host AZUREVM2 on Microsoft Hyper-V.</td>
</tr>
<tr>
<td>Information</td>
<td>08/22/2017 14:30</td>
<td>secRMM</td>
<td>300</td>
<td>secRMM: Device E: is OFFLINE in Virtual Machine host AZUREVM2 on Hypervisor host.</td>
</tr>
<tr>
<td>Information</td>
<td>08/22/2017 14:30</td>
<td>secRMM</td>
<td>400</td>
<td>Removable Media Security Audit: Drive E:; Volume: \Device\HarddiskVolume10, Description: Removable media detected in E:.</td>
</tr>
<tr>
<td>Information</td>
<td>08/22/2017 14:30</td>
<td>secRMM</td>
<td>402</td>
<td>Removable Media Security Audit: Drive E:; Volume: \Device\HarddiskVolume10, Description: Removable media detected in E:.</td>
</tr>
<tr>
<td>Information</td>
<td>08/22/2017 14:30</td>
<td>secRMM</td>
<td>402</td>
<td>Removable Media Security Audit: Drive E:; Volume: \Device\HarddiskVolume10, Description: Removable media detected in E:.</td>
</tr>
<tr>
<td>Information</td>
<td>08/22/2017 14:30</td>
<td>secRMM</td>
<td>402</td>
<td>Removable Media Security Audit: Drive E:; Volume: \Device\HarddiskVolume10, Description: Removable media detected in E:.</td>
</tr>
</tbody>
</table>
VBScript
The secRMM product uses a VBScript to send SCCM Status Messages to SCCM. The VBScript accepts parameters that allow you to list and delete the “secRMM SCCM Status Messages” in the SCCM database.

The screen shot below that shows the command to list the “secRMM SCCM Status Messages” to the screen (one page at a time).

The screen shot below that shows the command to list the “secRMM SCCM Status Messages” to a file.
Note that each record exported by the VBScript is contained in multiple lines. This may not be optimal but you are still able to perform string finds/searches on the data.

PowerShell

The secRMM product has a PowerShell script for processing secRMM events. One of the options of this PowerShell script is to retrieve the secRMM data from the “secRMM SCCM Status Messages” in the SCCM database.
The screen shot below that shows the command to list the “secRMM SCCM Status Messages” to the screen.

```
powershell ./GetSecRMMEvents.ps1
```

The screen shot below that shows the command to list the “secRMM SCCM Status Messages” to a file.

```
powershell ./GetSecRMMEvents.ps1 > c:\temp\secRMMSCCM_09262017.csv
```
The SQL command below retrieves the “secRMM SCCM Status Messages” directly from the SCCM database.

```
SELECT all
SMS_StatusMessage.Component,
SMS_StatusMessage.MessageID,
SMS_StatusMessage.MessageType,
SMS_StatusMessage.ModuleName,
SMS_StatusMessage.PerClient,
SMS_StatusMessage.ProcessID,
SMS_StatusMessage.RecordID,
SMS_StatusMessage.ReportFunction,
SMS_StatusMessage.Severity,
SMS_StatusMessage.SiteCode,
SMS_StatusMessage.SuccessfulTransaction,
SMS_StatusMessage.ThreadID,
SMS_StatusMessage.Time
FROM secRMM.
```
Troubleshooting

SCCM secRMM Console Extension

The SCCM secRMM Console Extension lets you centrally configure and deploy the secRMM rules/policies for the computers and users in your domain. Since this feature utilizes the base SCCM “Compliance Settings” component, the troubleshooting steps will be the same as any other “Compliance Settings” issue. The way to troubleshoot any SCCM issue begins with knowing which SCCM log files to look at. For “Compliance Settings” issues, you will need to look on an SCCM client computer (i.e. not the site server but a computer running the SCCM agent). The log files on the SCCM client computer are located at C:\Windows\CCM\Logs. For “Compliance Settings” issues, the log files you will want to look at are:

1. CIAgent.log
2. DCMAgent.log
3. DCMReporting.log
4. DcmWmiProvider.log
5. CIDownloader.log


If possible, use the CMTrace utility that Microsoft provides in the SCCM 2012 R2 Toolkit (the download is at http://www.microsoft.com/en-us/download/details.aspx?id=36213). Once you install the SCCM 2012 R2 Toolkit, CMTrace will be located in the C:\Program Files (x86)\ConfigMgr 2012 Toolkit R2\ClientTools directory.

CMTrace has a very nice feature where you can view several log files at once. To use this feature, go to File->Open on the main menu bar. The file open dialog will have a checkbox at the bottom of the dialog labeled “Merge selected files”. Make sure you select that and then Ctrl-Click the logs you want to look at (listed above).

When looking for errors, you can safely ignore the 2 errors from the CIDownloader.log that look like:

DeleteInstanceFromLantern failed (0x80041002).           CIDownloader
DCM::LanternUtils::DeleteAlreadyExistingModel - Failed to delete instance
PolicyPlatform_Policy.Name="Scopeld_..._Configuration_PolicyDocument",Authority="System Center Configuration Manager",Revision=3 (0x80041002).

SCCM secRMM User Policies

Validation
1. Login to a SCCM client workstation as one of the users in the SCCM User Collection you deployed the secRMM Policy to.
2. On the SCCM client workstation from step 1 above, as a local Administrator, open the “Computer Management” MMC and click the secRMM node.
3. On the right-hand side (i.e. the Actions column), click the “secRMM Configurations” Action.
4. You should see the userid (and corresponding user SID) from step 1 above in the “secRMM configuration” list.
   a. If the userid is in the “secRMM configuration” list from step 4 above, you can also verify the process by looking in the secRMM event log. In the secRMM event log, you will see an event id of 701. Look at the last line of the 701 event text. It will list the SCCM Compliance Setting properties: type, name and revision.
   b. If the userid is NOT in the “secRMM configuration” list, please follow the troubleshooting section directly below.

Troubleshooting

On the SCCM site server, open C:\Program Files\Microsoft Configuration Manager\Logs\SMSProv.log.
Find the string:
ExecQueryAsync: START SELECT CI_UniqueId FROM SMS_ConfigurationBaselineInfo WHERE LocalizedDescription like '% User - Removable Media Policy%' AND IsAssigned = 1

A few lines (5 lines) below that, you will see the SQL select statement that corresponds to the ExecQueryAsync command above. Note the record count is returned on the next line as well.

Execute SQL =select all SMS_ConfigurationBaselineInfo.CI_UniqueId from fn_ListConfigurationBaselineInfo_List(1033) AS SMS_ConfigurationBaselineInfo where (SMS_ConfigurationBaselineInfo.Description like N'% User - Removable Media Policy%' AND SMS_ConfigurationBaselineInfo.IsAssigned = 1)

If you have SQL Management Studio available, starting with the “select”, copy the SQL query above and paste it into a SQL query session that is mapped to your SCCM database. Ensure the record count matches what is listed in the SMSProv log.

If you do find errors in the log files mentioned above, please contact Squadra Technologies support and a support engineer will assist you in correcting the issue.
Known Issues

1. If you modify a secRMM policy (rules set), you must re-deploy the policy. We are looking into how to correct this behavior.
2. Do not use XML characters (&, >, <) in the secRMM policy description text. If you do, the policy generates an error when you save it. We are working to correct this issue.

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. The version of SCCM 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.

<table>
<thead>
<tr>
<th>Phone</th>
<th>562.221.3079 (United States and Canada)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td><a href="mailto:info@squadratechnologies.com">info@squadratechnologies.com</a></td>
</tr>
<tr>
<td>Mail</td>
<td>Squadra Technologies, LLC.</td>
</tr>
<tr>
<td></td>
<td>World Headquarters</td>
</tr>
<tr>
<td></td>
<td>7575 West Washington Ave. Suite 127-252</td>
</tr>
<tr>
<td></td>
<td>Las Vegas, NV 89128</td>
</tr>
<tr>
<td></td>
<td>USA</td>
</tr>
<tr>
<td>Web site</td>
<td><a href="http://www.squadratechnologies.com/">http://www.squadratechnologies.com/</a></td>
</tr>
</tbody>
</table>