Security Removable Media Manager

secRMMCentral

for AD domain environments

Version 9.9.21.0
(December 2019)

Protect your valuable data
# Contents

## INTRODUCTION

- Microsoft Event Forwarding .................................................. 5
- secRMMCentral Event Log .................................................. 5
- secRMMCentral Event Log Subscription .................................. 5
- Types of Event Log Subscriptions ........................................... 6
- Microsoft Event Forwarding references .................................... 6

## INSTALLATION USING ACTIVE DIRECTORY

- CREATE THE AD GPO ................................................................. 10
- Configure the “event collector” COMPUTER .................................. 14
  - Enable “event collector” permission to Event log ......................... 15
  - Install secRMMCentral on the “event collector” system .................. 16
  - Configure the Event Forwarding Subscription ............................ 19
  - Set the secRMMCentral event log to roll when full ....................... 20
  - Install secRMM on the event collector computer .......................... 21
  - Adjusting the security ....................................................... 21
    - Windows 10 ........................................................................ 21
    - Windows Server 2016 and above ............................................ 21

## VIEWING THE SECRMMCENTRAL DATA

- SHOW THE COMPUTER COLUMN ................................................ 22
- Viewing the “SOURCE EVENT” COMPUTERS .................................. 22

## USING THE SECRMMCENTRAL DATA

- MICROSOFT SYSTEM CENTER OPERATIONS MANAGER .................. 24
- STANDALONE SQL DATABASE FOR REPORTS ................................. 25
  - Prerequisites ........................................................................ 25
  - Setup .................................................................................. 25
  - Scheduled Task .................................................................... 32

## TROUBLESHOOTING

- .............................................................................................. 39

## CONTACTING SQUADRA TECHNOLOGIES SUPPORT

- .............................................................................................. 40
Introduction

Overview

secRMMCentral lets you collect the secRMM events from all the computers in your network into a central event log on a single computer. This is useful for environments that are not running Microsoft Operations Manager (or another similar systems management product) or if you need to implement fault-tolerant functionality for your removable media events. At a bare minimum, combined with the secRMM Excel AddIn, you can use secRMMCentral to centrally monitor and manage the secRMM product in your environment.

The remaining subsections in this section can be skipped and you can proceed directly to the “Installation using Active Directory” section if you are already familiar with the Microsoft Event Forwarding technology.

Architecture

Microsoft Event Forwarding

secRMMCentral is an implementation of the Microsoft Event Viewer Event Forwarding/Subscription technology. The Microsoft documentation uses the term “event collector” as the Windows computer that will receive the events (i.e. the central event log). The computers that forward the events (to the “event collector”) are called the “event source” computers. The “event source” computers are running the secRMM product and generating events into their local secRMM event log. The Microsoft Event Forwarding/Subscription technology relies upon the Microsoft WinRM technology. The section below (titled “Install/Configure WinRM”) will guide you through installing Microsoft WinRM if it is not already installed in your environment.

secRMMCentral Event Log

For secRMMCentral, we are going to create a new event log named secRMMCentral on the “event collector” computer. The event log named secRMMCentral will receive all the secRMM events from the “event source” computers. The “event collector” can act as both an “event collector” and an “event source” so if an end user uses the “event collector” computer to copy files to a removable media device, these events will be collected just like any other “event source” computer. Creating the secRMMCentral event log is done using a standard Windows Installation which will be downloaded from the Squadra Technologies web site.

secRMMCentral Event Log Subscription

Once the secRMMCentral event log is created, we will create an “event log subscription” on the “event collector” computer. The “event log subscription” tells the “event collector” computer (actually, the service running on the “event collector” computer named “Windows Event Collector” [Wecsvc]) which “event source” computers will participate, from what event log to collect events from (in our specific case, this will be secRMM), what event log to put them in (in our specific case, this will be secRMMCentral) and how the event log data will be forwarded (either push [called Source-initiated] or pull [called Collector-initiated]) to the “event collector” computer.
Types of Event Log Subscriptions

Microsoft lets you associate the “event source” computers to the “event collector” computer in two different ways:

1. Source-initiated subscriptions
2. Collector-initiated subscriptions

When you define a Source-initiated subscription, you use an Active Directory (AD) Group Policy Object (GPO) to tell the event log subscription on the “event collector” computer what computers are the “event source” computers. This is recommended if you have many computers in your network and they all have secRMM deployed on them. The Source-initiated subscription uses a “push” architecture.

When you define a Collector-initiated subscription, you manually add the computers to the event log subscription on the “event collector” computer. This is recommended if you only have a small number of computers in your environment. The Collector-initiated subscription uses a “pull” architecture. For the collector-initiated subscription, there is a configuration difference based on if your computers are in a domain or workgroup. We will point out these configuration differences in the installation steps below.

Microsoft Event Forwarding references

Before moving on to the installation, it might be beneficial to first read the following Microsoft links to increase your understanding of the Microsoft event forwarding technology:


Microsoft WinRM Overview

Supported Operations System Versions for WinRM


Microsoft versions of WinRM
If you are using the older Operating Systems (Windows XP with SP2, Windows Server 2003 with SP1, Windows Server 2003 with SP2, or Windows Server 2003 R2) and have already deployed WinRM 1.1, you need to decide whether you want to upgrade the WinRM 1.1 deployment to WinRM 2.0 first. You can choose not to upgrade to WinRM 2.0 (from WinRM 1.1), just be sure you enable the WinRM “EnableCompatibilityHttpListener” property when you configure WinRM in the section below. WinRM1.1 used (uses) ports 80 and 443 while WinRM2.0 uses 5985 and 5986 (for HTTP and HTTPS respectively). This impacts the WinRM service listener as well as the Windows Firewall settings. Compatibility between WinRM 2.0 and WinRM 1.1 is possible by using WinRM compatibility listeners (please read [http://blogs.msdn.com/b/wmi/archive/2009/07/22/new-default-ports-for-ws-management-and-powershell-remoting.aspx](http://blogs.msdn.com/b/wmi/archive/2009/07/22/new-default-ports-for-ws-management-and-powershell-remoting.aspx)). Note also that WinRM 2.0 requires the .Net 2.0 sp1 framework (at a minimum).

![Software Update Installation Wizard](image)

Figure 1 - Install WinRM 2.0 on older Windows OS

Lastly, Windows 8 and better are using WinRM 3.0. WinRM 3.0 and WinRM 2.0 appear to coexist without any need for special configuration.

**Detecting which version of WinRM is installed**

WinRM service is running

If the WinRM service is running, from an elevated command prompt, type: `winrm id` and then look in the table below using the first part of the ProductVersion line in the output.
Figure 2 - Checking the WinRM version using WinRM command

Note: If you get an access denied error when you issue winrm id (see screen shot below), be sure that the Administrator userid you are using has a password. Also, issue the following command so that your local Administrator account can get past User Access Control (UAC):

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

If you still get an error after the steps above, then you should go to the section below titled “Install/Configure WinRM” to issue the command `winrm quickconfig` since it is likely that winrm has not yet been configured on the computer.

Figure 3 - Access denied error issuing WinRM command due to UAC

WinRM service is not running

If the WinRM service is not currently running, you can determine the version of WinRM installed on your system by checking the version of the file `%Windir%\System32\wsmsvc.dll`. You need to use Windows Explorer to do this. Using Windows Explorer, right mouse click on `%Windir%\System32\wsmsvc.dll` and select the Properties menu item. In the tabbed Properties window, click the Details tab. Look at the Property named “Product version”. The table below outlines the WinRM version number that is indicated by the various possible file version numbers of `%Windir%\System32\wsmsvc.dll`:

<table>
<thead>
<tr>
<th>Version number for <code>%Windir%\System32\wsmsvc.dll</code></th>
<th>WinRM version</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.3790.2075</td>
<td>0.5</td>
</tr>
<tr>
<td>6.0.6000.16386</td>
<td>1.0</td>
</tr>
<tr>
<td>5.1.2600.3191</td>
<td>1.1</td>
</tr>
<tr>
<td>5.2.3790.2990</td>
<td>1.1</td>
</tr>
</tbody>
</table>
Microsoft WinRM references

Before moving on to the installation, it might be beneficial to first read the following Microsoft links to increase your understanding of the Microsoft WinRM technology:

Installation and Configuration for Windows Remote Management at:

Details on the changes in Windows Remote Management behavior in Windows Server 2008 R2 and Windows 7

Comments about WinRM

We chose to use the Microsoft Windows Event Forwarding technology since it comes as a core component of the newer Microsoft Operating Systems. The steps to setup the Event Forwarding Technology are not difficult. We wish that could be said of WinRM. WinRM is not difficult to install if your environment is entirely comprised of the newer Microsoft Operating Systems and you are running in a domain environment. In this case, you can simply use Active Directory Group Policy to install and configure WinRM. Where it becomes more challenging is when you also are still running the older Microsoft Operating Systems and have already deployed WinRM version 1.1. Installing WinRM in a non-domain (i.e. WORKGROUP) environment also requires additional steps. In this document, we give you all the commands you need to handle a mixed WinRM versioned environment and for a non-domain environment. All that said, there are security considerations that need to be made. While we make every attempt to answer these questions in this documentation, you will need to factor in the security policies of your environment and weave them into the steps in the Installation sections below. Squadra Technologies is always willing to provide free technical support during the secRMMCentral deployment so if you have questions and need assistance, please call us.

With all that said, you might be somewhat hesitant about using WinRM. However, the advantages of using this technology, combined with Windows Event Forwarding technology make it attractive to implement. First off, since these technologies come as part of the OS, there is no agent needed (although running the WinRM service could be argued that it is an agent). The solution is very scalable and the collector is capable of supporting 100s or 1000s of computers. If you are working in a domain, Microsoft has made the configuration available in Active Directory Group Policy. This is useful in a large
deployment. Finally, a huge benefit of the Microsoft Event Forwarding technology is for systems that are mobile (i.e. sometimes on the network and sometimes not on the network), the Windows Event Forwarding technology will pick up all the events once the system comes onto the network.

**Installation using Active Directory**

The following sections describe how to deploy WinRM, Microsoft Event Forwarding and secRMMCentral. These 3 components are all inter-related to allow you to forward the secRMM events from all the computers in your environment into one computer's event log (this event log will be named secRMMCentral and the computer is the “event collector”).

Before you start, you will need to choose a computer in your environment that will act as the “event collector” (i.e. the computer that will receive all the forwarded secRMM events). This computer is where you will install secRMMCentral.

Since the Microsoft Event Forwarding technology relies on WinRM. WinRM must be installed and configured on both the “event collector” and “event source” computers. These steps are outlined below.

**NOTE:** If your domain controller is not yet on W2008 and you do not see the “Windows Remote Management” System Service in step 1 below, you can download the Windowsremotemanagement.adm from [http://support.microsoft.com/kb/936059](http://support.microsoft.com/kb/936059).

**Create the AD GPO**

Using the Group Policy Management MMC, create a Group Policy Object with the following 4 settings:

1. Set the WinRM service to auto start:
   
   A. In the Group Policy Editor, navigate to Computer Configuration \ Policies \ Windows Settings \ Security Settings \ System Services.
   
   B. Double click Windows Remote Management (WS-Management)
   
   C. Set it to Automatic.
2. Create the WinRM listener:

   A. In the Group Policy Editor, navigate to Computer Configuration \ Policies \ Administrative Templates \ Windows Components \ Windows Remote Management (WinRM) \ WinRM Service.

   B. Double click:

      a. For pre-W2012: Allow automatic configuration of listeners
      b. For W2012: Allow remote server management through WinRM

   C. Set the IPv4 and IPv6 filters to * (an asterisk).

   D. [Optional] If you have any older Windows systems using WinRM 1.1 AND they are still using the old WinRM service listener port numbers (i.e. 80 and 443), then you should also enable “Turn On compatibility HTTP[S] Listener”
3. Create a firewall exception for WinRM:

   A. In the Group Policy Editor, navigate to Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Windows Firewall with Advanced Security \ Inbound Rules.

   B. Create an Inbound Rule for WinRM for port 5985. Select the “Predefined” radio button and select the “Windows Remote Management” in the drop-down listbox.

Note: The firewall rule you create in the GPO (above) equates to the command line:

```
netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-In)"
dir=in action=allow service=any enable=yes profile=any localport=5985 protocol=tcp
```
4. Specify the “event collector” computer for the “event source” computers

A. In the Group Policy Editor, navigate to Computer Configuration \ Policies \ Administrative Templates \ Windows Components \ Event Forwarding.
B. Double click either (whichever is listed in your environment):
   a. Configure target subscription manager
   b. Configure the server address
C. Click the Enable button.
D. Click the Show button (to the left of the button, it says subscription managers)
E. Add the value Server=TheCollector.YourDomain.com
   a. Where TheCollector.YourDomain.com is the FQDN name of the “event collector” computer in your environment
   b. NOTE: Make sure you type in the “Server=” text

Figure 7 - Group Policy Object for the event forwarding subscription
Figure 8 - Group Policy Object for the event forwarding subscription -> specifying the "event collector" computer

Configure the “event collector” computer

To configure the “event collector” computer:

1. You must login to the “event collector” computer using an Administrators account.

2. Open a Command Prompt Window in Administration Mode

   a. At the command prompt, type `winrm qc`

   b. At the command prompt, type: `wecutil qc`
3. Respond Y if you get the prompt in the screen shot below.

Enable “event collector” permission to Event log

Add the “Network Service” built-in user account (i.e. not from the domain but from the local computer) to the “Event Log Readers” Group.
Install secRMMCentral on the “event collector” system

1. On the “event collector” system, download the secRMMCentral installation program from the Squadra Technologies web site at http://www.squadratechnologies.com/Products/secRMM/secRMMDownloads.aspx. The secRMMCentral download is under the “Additional optional downloads” link on the Squadra Technologies download page.

---

Figure 12 - Add network service built-in account to Event Log Readers group

---

<table>
<thead>
<tr>
<th>Item</th>
<th>Download link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft System Center/Azure</td>
<td>secRMM System Center/Azure</td>
</tr>
<tr>
<td>Excel AddIn</td>
<td>secRMMExcelAddIn</td>
</tr>
<tr>
<td>secRMMCentral</td>
<td>secRMMCentral</td>
</tr>
</tbody>
</table>
secRMMCentral collects all the secRMM events from the computers running secRMM. This might be necessary if you are not using Microsoft Operations Manager or another systems management product.

secRMMCentral utilizes Microsoft Windows Event Log Forwarding/Subscriptions. This Microsoft technology allows you to define a central repository of events from other computers. secRMMCentral works with the secRMM Excel AdIn to allow you to look at an individual system or all the systems in your environment.

<table>
<thead>
<tr>
<th>Item</th>
<th>Download link</th>
</tr>
</thead>
<tbody>
<tr>
<td>secRMMCentral x64 install</td>
<td>secRMMCentralInstallx64.zip</td>
</tr>
<tr>
<td>secRMMCentral x66 install</td>
<td>secRMMCentralInstallx86.zip</td>
</tr>
<tr>
<td>Administrators Guide</td>
<td>secRMMCentralAdministratorGuide.pdf</td>
</tr>
</tbody>
</table>
|                    | left click to view online
|                    | right click and then "Save As" to download |

Figure 13 - Download secRMMCentral installation from Squadra Technologies web site

2. Perform the secRMMCentral installation **only on** the “event collector” system:
3. Once the installation is complete, you will see the secRMMCentral event log in the event log viewer:
Configure the Event Forwarding Subscription

In the secRMMCentral installation directory on the “event collector” computer (you performed this installation in the previous section), there is an XML file that get installed called: SubscriptionSourceInitiated.xml
Using a CMD window in Administrator mode, change into the directory where secRMMCentral is installed (this is C:\Program Files\secRMMCentral by default) and execute the SubscriptionSourceInitiated.cmd. This cmd file will use the xml file SubscriptionSourceInitiated.xml to create the subscription.

**Set the secRMMCentral event log to roll when full**

Right mouse click on the secRMMCentral event log and select “Properties”. In the “General” tab, set “Archive the log when full, do not overwrite events”. 
Install secRMM on the event collector computer

Next, make sure you have secRMM (i.e. the core product, i.e. secRMMInstallx64.msi or secRMMInstallx86.msi) installed on the “event collector” computer.

Adjusting the security

Windows 10

If your “event collector” computer is running Windows 10, you will need to modify the permissions to allow the local network service to access the WinRM URL. Please enter the following command (try to use “cut and paste” to avoid mistyping the command):

```
netsh http add urlacl url=http://+:5985/wsman/ user="NT AUTHORITY\NETWORK SERVICE"
```

Windows Server 2016 and above

If your “event collector” computer is a Windows Server version 2016 and above, you will need to modify the permissions to allow the local network service to access the WinRM URL. Please enter the following commands (try to use “cut and paste” to avoid mistyping the commands):

```
netsh http delete urlacl url=http://+:5985/wsman/


netsh http delete urlacl url=https://+:5986/wsman/


netsh http show urlacl
```

Details about the commands listed above are in the following Microsoft KB article:


Viewing the secRMMCentral data

Now that the installation is complete, you will start to see the secRMM events from the “source event” computers showing up in the secRMMCentral event log on the “collector event” computer.
Show the Computer column

You can right mouse click on any column header (ex: Level, ‘Date and Time’, etc.) and select ‘Add/Remove columns…’. Click ‘Computer’ in the ‘Available columns’ list and then click the ‘Add’ button so that the ‘Computer’ column shows in the ‘Displayed columns’ list.

Viewing the “source event” computers

On the secRMMCentral (collector) computer, within the “Event Viewer”, you can see the “source event” computers as shown in the screenshot below. Notice the column labeled “Source Computers”. It shows the number of “source event” computers that are registered with the “collector computer” (i.e. secRMMCentral).
When you click the secRMMCentral subscription, the Actions column will give you options to further see your environment as shown in the screenshot below.

The “Runtime Status” is especially useful since it will show you the list of “source event” computers and their current status (green icon means it is connected to the collector computer).

If you are first bringing on “source event” computers and they are not “Active”, try restarting the WinRM service on the “source event” computer. This will usually bring it to the “Active” Status.
Using the secRMMCentral data

Microsoft System Center Operations Manager

secRMMCentral has a System Center Operations Manager (SCOM) Management Pack available. The SCOM Management Pack allows you to see the secRMMCentral events as SCOM alerts. It also gets the secRMMCentral events into the SCOM databases (Datawarehouse and ACS) for reporting purposes. To get the secRMMCentral SCOM Management Pack, please go to http://www.squadratechnologies.com/Products/secRMM/SystemCenter/secRMMSystemCenterOperationsManager.aspx.

<table>
<thead>
<tr>
<th>Item</th>
<th>Download link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft System Center Operations Manager secRMM Management Pack</td>
<td>Squadra.secRMM.xml</td>
</tr>
<tr>
<td></td>
<td>right click and then &quot;Save As&quot; to download</td>
</tr>
<tr>
<td>Microsoft System Center Operations Manager ACS and Data Warehouse reports</td>
<td>secRMMReports</td>
</tr>
<tr>
<td>Microsoft System Center Operations Manager Administrators Guide</td>
<td>secRMMSCOM.pdf</td>
</tr>
<tr>
<td>Microsoft System Center Operations Manager secRMMCentral Management Pack</td>
<td>Squadra.secRMMCentral.xml</td>
</tr>
<tr>
<td></td>
<td>right click and then &quot;Save As&quot; to download</td>
</tr>
</tbody>
</table>
Standalone SQL database for reports

If you do not have a backend framework product (such as SCCM or SCOM or a SIEM tool) that can consume the secRMMCentral event data, you can still generate reports from the data using a standalone SQL database. If possible, the SQL instance should be on the same computer as the secRMMCentral event log (which you setup above). While it is possible for the SQL instance to be on a separate computer, you will need to edit some of the installation scripts (in the instructions below). If your SQL instance is on a separate computer from the secRMMCentral event log, please contact Squadra Technologies support for assistance.

Prerequisites

You will need the following software components installed:

1. Microsoft SQL server with the “SQL reporting services” component installed
2. Microsoft Command Line Utilities for SQL Server (i.e. sqlcmd)
3. Microsoft Log Parser
4. Squadra Technologies secRMM (i.e. the core product, i.e. secRMMInstallx64.msi or secRMMInstallx86.msi)
5. Microsoft SQL Management Studio (optional but very helpful)

Setup

1. Download the secRMMStandaloneReports.zip file from the Squadra Technologies web site under the secRMM Download area as shown in the screenshot below
2. Unzip the secRMMStandaloneReports.zip file. It is recommended that you unzip it in the secRMMCentral directory as shown in the two screenshots below.
3. 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.
4. Within the secRMMStandaloneReports subdirectory, edit CMD file Standalone_ImportSecRMMEventsIntoSQL.cmd to set the variables below for your environment:
   Line 33: set SQLServerAndInstance=localhost
   Line 34: set DatabasePhysicalFilesLocation=C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\n   Line 35: set DatabasePhysicalFilesLocationLog=C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\
5. Run Standalone_ImportSecRMMEventsIntoSQL.cmd so that the SQL database named secRMMDatabase gets created.
6. Once the database named secRMMDatabase exists, register the .net assemblies named secRMMSQLScalarValuedFunction and secRMMSQLTableValuedFunction.dll into the SQL database named secRMMDatabase by running the script InstallAssemblyForStandaloneDB.cmd in the Assembly subfolder.
7. Run the following SQL query against the secRMMDatabase (preferably using SQL Management Studio):
   
   ```sql
   select * from dbo.secRMMSQLTableValuedFunction(N'Standalone',0)
   ```
   
   Make sure there are no errors reported.

8. If you already have a secRMMCentral event log on the system, run
   BackupSecRMMCentralEventLog.cmd to verify that it generates a "backup evtx file for the secRMMCentral event log" into this directory (i.e. the directory where this Standalone_README.txt file resides...by default, this will be C:\Program Files\secRMMCentral\secRMMStandaloneReports).

9. When there is one or more .evtx file(s) in the directory, run the script
   Standalone_ImportSecRMMEventsIntoSQL.cmd. **Note:** that we have seen times where you need close SQL Management Studio before this command will complete. It seems that some SQL lock gets created that hangs the script caused by the LogParser utility

10. Verify that there is now data in the secRMMDatabase table named secRMMTable

11. Run the following SQL query against the secRMMDatabase (preferably using SQL Management Studio):
    
    ```sql
    select * from dbo.secRMMSQLTableValuedFunction(N'Standalone',0)
    ```
    
    Verify there is data output.

12. In the command window, change directory (CD) into the Reports\STANDALONE sub-directory.

13. In the Reports\STANDALONE sub-directory, you will see a file named ImportReports.cmd and ImportReports.ps1 (as shown in the screenshot below).
14. In the command window, type `ImportReports.cmd` and hit the enter key. The output will look similar to the screenshot below.

![Command Prompt Output](image)

15. You can now run the reports by opening a browser.

16. Go to the URL: [http://localhost/reports](http://localhost/reports)

![Browser Screenshot](image)

17. Click into the “Removable Media Security” folder within the browser.

![Removable Media Security Folders](image)

18. Click any one of the reports to run them.
Scheduled Task

You should create a scheduled task that will take the events from the secRMMCentral event log and put them into the SQL secRMMDatabase. It is up to you how often you want to run the scheduled task but once a day is a good value. The action that the scheduled task should take is to call the script named C:\Program Files\secRMMCentral\secRMMStandaloneReports\ScheduledTask.cmd (see screenshot below).
1. Go to the Windows Task Scheduler (taskschd.msc)
2. Within the Windows Task Scheduler, go to the secRMM folder
3. In the Actions column, click “Create Basic Task…”

4. Specify the Name and Description and then click the next button.

5. Specify how often you want to run the scheduled task and then click the next button.
6. Specify the time to run the scheduled task and then click the next button
7. Specify “Start a program” and then click the next button
8. For the “Program/script”, specify:
"C:\Program Files\secRMMCentral\secRMMStandaloneReports\ScheduledTask.cmd"
For the “Start in (optional)”, specify:
C:\Program Files\secRMMCentral\secRMMStandaloneReports
9. Click the Finish button
Troubleshooting

If you have followed the steps explained in the sections above but are not getting events into the secRMMCentral event log, this section offers some troubleshooting steps. You may also want to contact Squadra Technologies technical support to get assistance.

1. Check the secRMM event log on the “event source” computer(s) to make sure there are current events. You can plug-in and remove a removable storage device to generate event ids 400 and 403.

2. On an “event source” computer, issue the WinRM commands below. Use the output of the command to determine if it was successful or an error occurred. The bold text is the text you will need to provide from your environment.

   ```
   winrm id -auth:none -remote:<hostname of the event collector machine>
   winrm id -remote:<hostname of the event collector machine>
   winrm get winrm/Config -r:<hostname of the event collector machine>
   ```

3. There are 3 Microsoft event logs that will help you to see if there are any WinRm errors. They are all under the Applications and Services Logs->Microsoft folder. They are listed below in the order in which you should look for errors:
   1. Eventlog-ForwardingPlugin
   2. Windows Remote Management
   3. Windows Firewall With Advanced Security
4. If one or more of the commands in step 2 failed or you are seeing errors in the events logs from step 3, determine if there is a proxy server between the event collector and the event source computer(s). You can use the tracert command to see the network hops. If there is a proxy server, you will need to modify WinRM (on the source computers) using the command:

```
netsh winhttp set proxy proxy-server=http://hostname of the proxy/
```

### Contacting Squadra Technologies Support

Squadra Technologies Support is available to customers who have purchased a commercial version of secRMM and have a valid maintenance contract or who are in a trial mode of the product. When you contact Support please include the following information:

1. The version of secRMM you have installed.
2. The Windows versions you have installed: XP, 2003 Server, 2008 Server R2, Vista, Windows 7, etc.
3. Whether the Windows Operating System is 32bit or 64bit.
4. The specific issue you are contacting support for.

### About Squadra Technologies, LLC.

Squadra Technologies delivers innovative products that help organizations get more data protection within the computer infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Squadra Technologies is helping customers worldwide.

Contacting Squadra Technologies, LLC.

- **Phone**: 562.221.3079 (United States and Canada)
- **Email**: info@squadratechnologies.com
- **Mail**: Squadra Technologies, LLC.
  World Headquarters
  7575 West Washington Ave. Suite 127-252
  Las Vegas, NV 89128
  USA