Security Removable Media Manager

Administrator Guide

Version 9.0.0.0

(March 2016)

Protect your valuable data

If you have any questions regarding your potential use of this material, contact:

Squadra Technologies, LLC
7575 West Washington Ave
Suite 127-252
Las Vegas, NV 89128 USA
www.squadratechnologies.com
email: info@squadratechnologies.com

Refer to our Web site for regional and international office information.

TRADEMARKS

Disclaimer

Squadra Technologies Administrator Guide
Created - March 2011

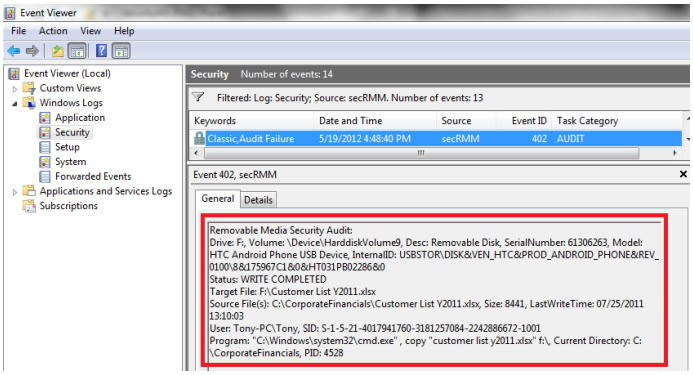
Contents

Introduction

Squadra Technologies *security Removable Media Manager* (**secRMM**) software is Windows security software that runs on your company's workstations and servers. secRMM manages and monitors removable media. In this context, Removable media is defined as external hard disks, USB (flash) drives, smart phones, tablets, SD-Cards, CD-ROM and DVD. Generally, any storage device that supports Microsoft plug-and-play will be managed and monitored by secRMM. Such devices typically use the computers Universal Serial Bus (USB) ports to connect to the computer. Removable media devices are popular because they are very convenient when you want to copy files around or backup data. secRMM allows you to track all write activity to the removable media devices in your computer environment as well as giving you the ability to control (or authorize) who can write to the removable media devices.

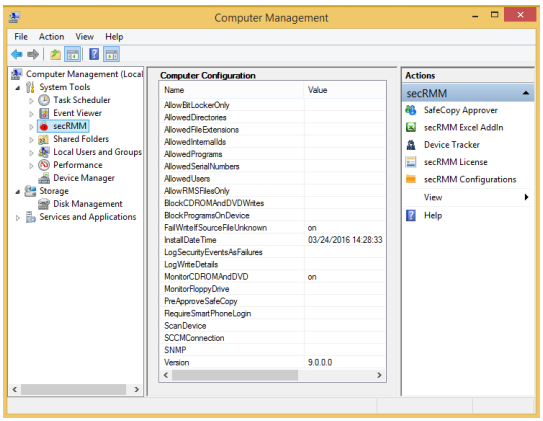
Features

Detailed forensic data for smart phones, tablets and removable media



secRMM monitors and collects very detailed forensic data about removable media write activities. This ensures that if a security incident does occur and removable media is involved, you will be able to understand the exact nature of the security incident. The level of detail collected by secRMM is what distinguishes secRMM from other products that attempt to provide similar functionality. Surprisingly, other competing solutions are not even able to report the complete file path of the files being copied from the local computer and/or network. Missing this important data makes the security forensic data incomplete and will make any security analysis exercise a guessing game. secRMM was developed to address requirements coming from the United States government and military organizations. This means secRMM ensures that removable media write activity is always predictable and the events are always captured to a nonrepudiation store (i.e. the Windows Security event log).

Useful yet simple authorization modules



secRMM provides a removable media authorization layer to prevent any removable media security incidents from ever occurring in the first place. Unlike other competing solutions, secRMM lets you control what files the end-user can copy from the local computer and/or network. The other authorization modules let you control removable media write activity based on userid, removable media serial number, removable media internal Ids (i.e. VIDs and/or PIDs) and the program used to perform the write operations

to the removable media.

Prevent unauthorized devices from mounting

secRMM can prevent unauthorized devices from mounting to the Windows Operating System. The advantage of using this feature is that even though the device cannot be read from or written to, the device still receives power from the Windows computer. This allows your end-users to still charge their device (usually a smart phone or tablet) while keeping the data in your environment safe. A corresponding event is generated when this even occurs so you can know who is charging their phone or tablet. This feature is available on the device serial number, the device internal ID (VID/PID) and for userids.

Smart phone app for added security

For heightened security environments such as military and/or government, secRMM comes with a mobile (smartphone/tablet) app that forces the end-user to login (authenticate) from the mobile device before the device will appear as a USB storage device to Windows. Note that you are not required to use this feature; it is an optional security feature. The secRMM mobile app is available in the Android, Apple, BlackBerry and Windows app stores.

Enforceable two man policy

secRMM comes with an end-user GUI application called SafeCopy that works in conjunction with secRMM. The SafeCopy user interface mimics the standard Windows explorer program but only allows writing to removable media and adjusts what it displays to the end-user based on secRMM properties. Administrators can easily enable secRMM/SafeCopy to enforce a two man policy. A two man policy means at least 2 people must be involved for the removable media write operation to occur. The two man policy is a common operating procedure in many critical government and military situations. The secRMM/SafeCopy two man policy implementation allows administrators to monitor each operation the end-user takes while using the SafeCopy program. A check is made if an administrator tries to approve himself. This check will not allow the approval.

Removable Media device tracking

If you configure secRMM so that your end-user must use secRMM SafeCopy to copy file(s) to removable media devices, secRMM puts a small signature onto the removable media device. This gives you the ability to see who the last user was to use a removable media device. This can be a powerful feature for lost or stolen removable media devices.

Transparent integration with hardware/software encryption technology

secRMM works seamlessly with hardware and software encryption technologies. In fact, secRMM generates the necessary security events required:

1. An event telling you that an encryption device has been plugged into the Windows computer (i.e. mounted)
2. An event telling you that the authorization to use the device has succeeded. Encryption technology authorization is done using either software (i.e. a dialog asking for your password) or hardware using a push button key pad. Examples of software authorization include IronKey device and Microsoft BitLocker. An example of hardware authorization is the Apricorn Aegis Secure Key USB Flash Drive.

Light-weight

secRMM is designed as a light-weight security software product. What this means is that when secRMM does not need to be running, it enters into a quiescent state. The secRMM software will run only when a Removable Media device is plugged into the computer. This means that your end-users will not feel a performance impact from the secRMM software in their normal day-to-day computer work activities.

Tightly integrated with Microsoft Windows Operating System

secRMM was designed to fit into the most common security and monitoring scenarios. This means secRMM utilizes Microsoft best practices by utilizing core Windows Operating System components rather than writing a separate framework to monitor Removable Media devices. The benefit to this approach is that secRMM does not require a large learning curve or large setup period. It also means you can integrate secRMM into your existing security and monitoring strategies/implementations with very little work. secRMM uses the familiar Microsoft Management Console (MMC) as the User Interface (UI) to make secRMM configuration changes.

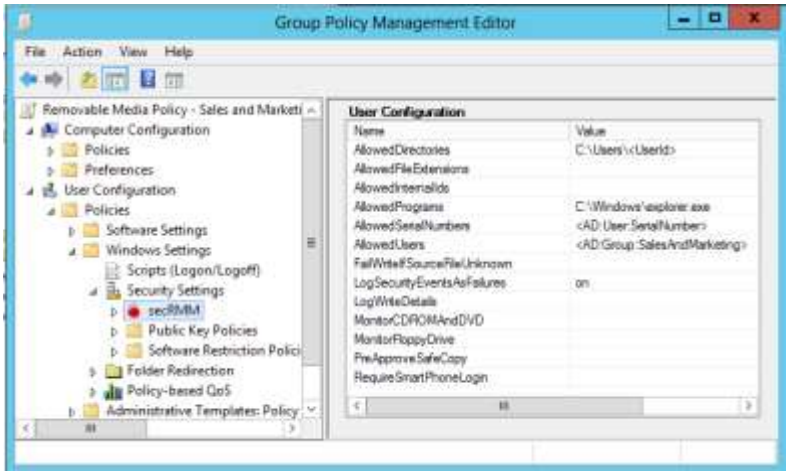
100% scriptable

In addition to the MMC User Interface, secRMM can be controlled and configured using any Microsoft COM compatible scripting language (i.e. Powershell, VBScript, Jscript, Perl) as well as any .Net language. For more details, please review the section titled "Integrating secRMM into your environment".

SetAllowedInternalIds.vbs

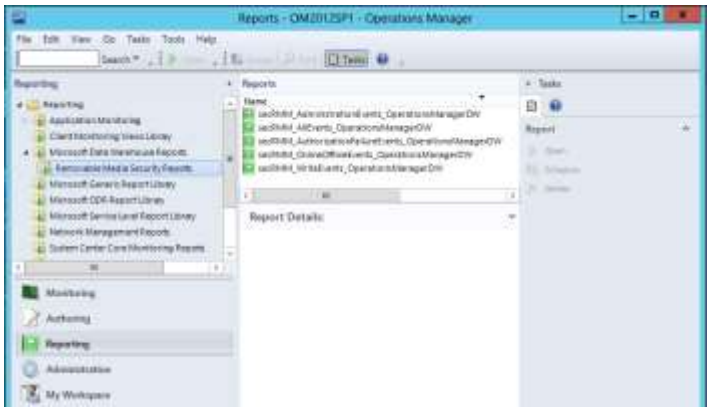
```
'*********************************************************************
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "AllowedInternalIds", "VID_04e8&PID_6860"

'To turn this feature off, use the line below instead of the line above
'objSecRMM.SetProperty "AllowedInternalIds", Null
```

Tightly integrated with Microsoft Active Directory



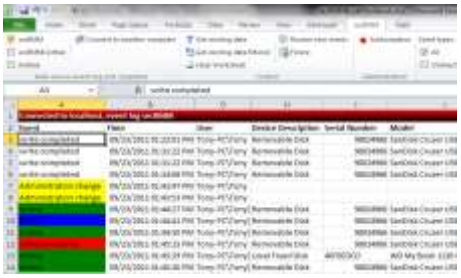
secRMM takes advantage of Active Directory in two powerful ways. First, secRMM properties can be applied using Active Directory Group Policy. The Group Policy Editor has both a computer and user configuration security settings secRMM node. The user interface for the Group Policy Editor is identical to the secRMM user interface in the Computer Management MMC. This means secRMM security settings can be applied to the computer, a group of users and/or individual users. Secondly, secRMM can use Active Directory computer object and user object attributes within the secRMM properties (AllowedDirectories, AllowedSerialNumbers and AllowedUsers). This makes applying removable media security policies very easy to maintain and deploy.

Tightly integrated with Microsoft System Center



Because secRMM does not use a proprietary framework to function, secRMM easily integrates into the system management tools used within any environment. Microsoft System Center is the dominant systems management tool on the market today. secRMM has integration with SCCM (installation, configuration, status messages and reports), SCOM (events, alerts, tasks and data warehouse/ACS reports) and Orchestrator.

Tightly integrated with Microsoft Excel 2010



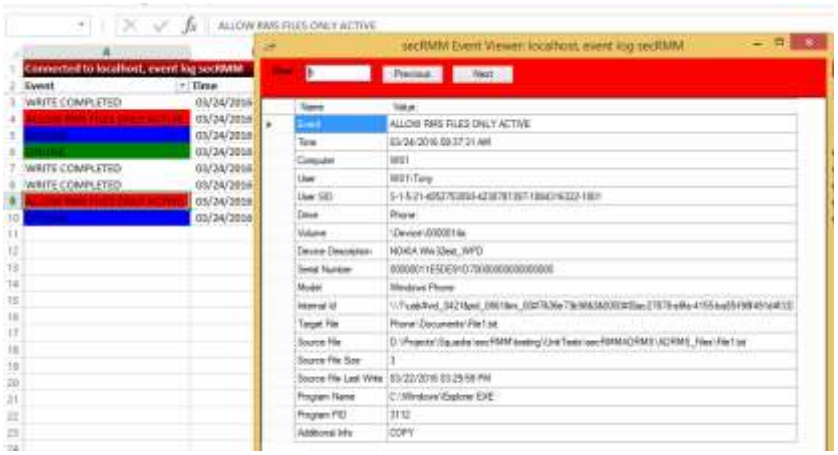
secRMM comes with an Excel AddIn[1] that makes analysis, filtering and reporting very simple.

[1] For details please review the "secRMM Excel AddIn Administrators Guide" from the Squadra Technologies web site.

Tightly integrated with Microsoft Azure, Hyper-V and RDP

secRMM supports USB drives that are available to remote machines under Azure and Hyper-V via the Remote Desktop RemoteFX USB redirection feature. This feature even works when you use a Remote Desktop session to another physical computer. The secRMM online events contain information about the Hypervisor server and the remote machine. The event data gets logged in both the physical and remote secRMM event logs. This gives you a complete picture of your removable storage within your domain whether it exists on premise or in the cloud. This feature requires you to have secRMM running on both the RDP client and the RDP server.

Tightly integrated with Microsoft Rights Management Services



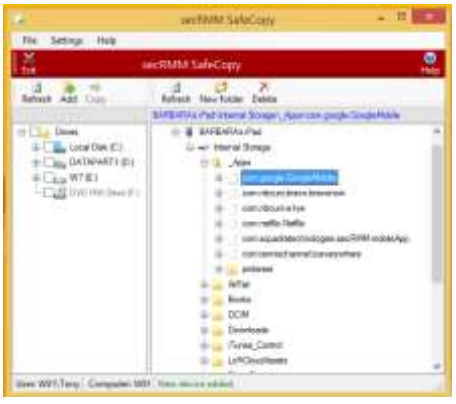
secRMM works in conjunction with Microsoft Rights Management Services (RMS). You can specify a secRMM rule that will only allow files protected with Microsoft RMS to be copied to removable storage devices.

Microsoft RMS is a powerful security technology that allows the security of the data to be self-contained with the file.

Microsoft RMS must be setup in your domain, it is not available by default.

For Microsoft documentation on RMS, please see https://technet.microsoft.com/en-us/library/cc771234(v=ws.10).aspx.

Copy files to/from apple mobile devices



secRMM comes with apple mobile device functionality that lets you copy files to/from to apple mobile devices file system. This functionality is integrated into the secRMM SafeCopy program. SafeCopy exposes the entire apple file system including the sandboxed Apps data directories. If you want to make your own apple program, you can use the secRMM SDK. The secRMM SDK allows you to integrate any mobile device into your enterprise. Note, that starting with IOS 8.3, Apple has unfortunately locked down the App data directories unless the App was built with the UIFileSharingEnabled flag set.

Flexible licensing

secRMM has 4 different license modes:
1. Freeware – the freeware version logs online and offline removable media events.
2. By computer – secRMM provides all features in this licensing mode.
3. Domain – secRMM provides all features in this licensing mode.
4. Forest – secRMM provides all features in this licensing mode.

Modes of operation

secRMM has 4 modes of operation: Monitoring, Authorization, Lockdown and Eject.

Monitoring mode

Monitoring mode records (via the Windows event log component) all Removable Media write activity (as well as when a Removable Media device comes online and offline). Monitoring mode is always on and cannot be turned off. When you perform a "typical" (as opposed to a custom) secRMM installation, monitoring mode is running after the installation. When secRMM is in authorization, lockdown or eject mode, monitoring mode is still on as well.

Authorization mode

Authorization mode is when you want to limit who or what program can perform write activity to the Removable Media. In addition to who or what (program), you can also limit Removable Media write activity based on the Removable Media device's serial number(s) and/or the device's internal Id (VIDs/PIDs), the source directory(ies) and by file extension(s). Authorization mode starts when you specify one of the secRMM whitelisting properties. The secRMM whitelisting properties are: AllowBitLockerOnly, AllowedDirectories, AllowedFileExtensions, AllowedInternalIds, AllowedPrograms, AllowedSerialNumbers, AllowedUsers. All of these properties are detailed below.

Lockdown mode

Lockdown mode prevents any write activity to Removable Media. Lockdown mode is really a special version of Authorization mode. The difference is that lockdown mode sets the secRMM "AllowedSerialNumbers" property to a value that is a nonexistent serial number (the value is secRMM_is_locked_down) so the Removable Media write activity (no matter what device) will always fail.

Eject mode

Eject mode checks the device serial number, the device internal id and the logged in users against the secRMM authorization properties of the same name. If there is a mismatch, secRMM ejects the device so that to the end-user, the device appears to have never been mounted by the Windows operating system.

Eject mode differs from authorization/lockdown mode because it happens when the device is coming online vs. when a write operation occurs.

Monitoring mode

The secRMM product logs 4 distinct events for monitoring. The 4 secRMM events are described and shown in screenshots below.

Online/Offline events

The secRMM product logs when a Removable Media device is plugged in (an online event) and when a Removable Media device is removed (an offline event). The online and offline secRMM events list the device and all users who are currently logged into the computer at the time the event occurred. The secRMM online event has an event id of 400 (see Figure 1). The secRMM offline event has an event id of 403 (see Figure 2).

Details

Line 1: Removable Media Security Audit:
Line 2: Drive: F:, Volume: \Device\HarddiskVolume9, Desc: Removable Disk, SerialNumber: 61306263, Model: HTC Android Phone USB Device, InternalID: USBSTOR\DISK&VEN_HTC&PROD_ANDROID_PHONE&REV_0100\8&175967C1&0&HT031PB02286&0
Line 3: Status: ONLINE
Line 4: User(s): Tony-PC\Tony[Interactive]

Line 1	Indicates that this event is from secRMM.
Line 2	Describes the Removable Media device. Listed is the drive letter or name of the device assigned by the operating system, the volume name, a brief description of the device, the manufacturer assigned serial number, the manufacturer model information and the devices internal ID.
Line 3	The status of the device. This value will be either ONLINE or OFFLINE.
Line 4	The users who are logged onto the computer at the time of the event.

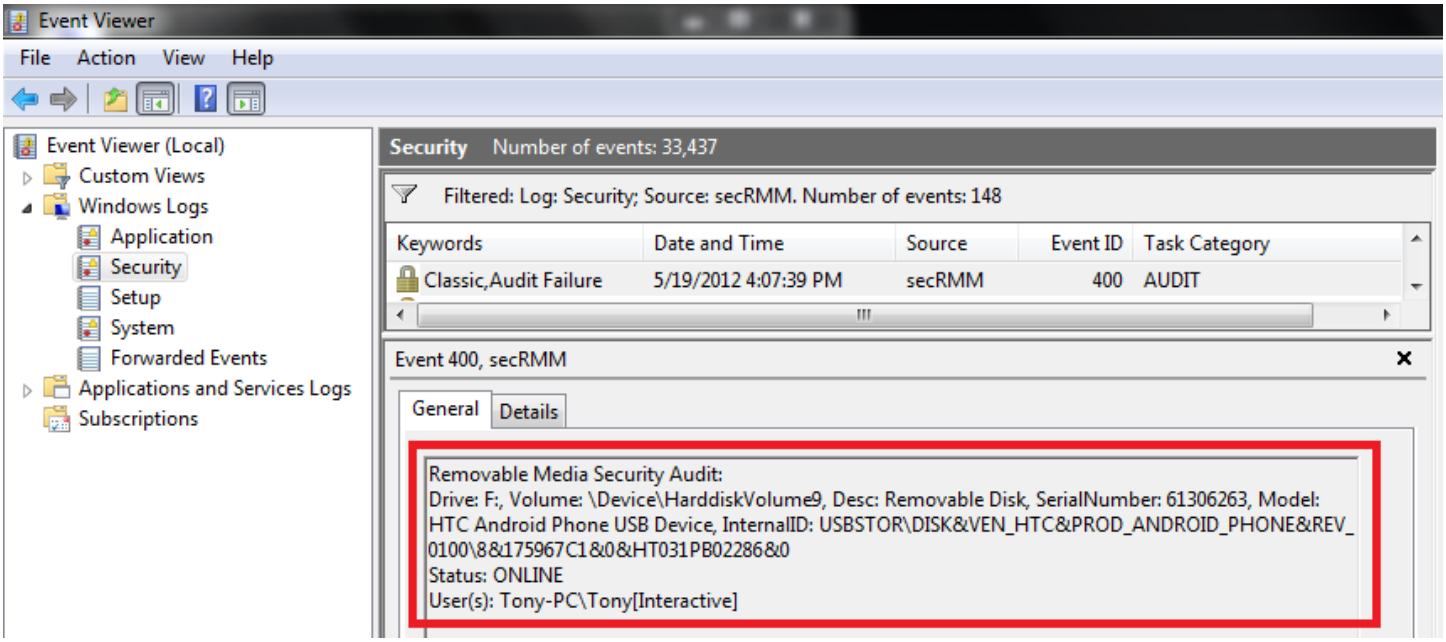


Figure 1 – secRMM online event

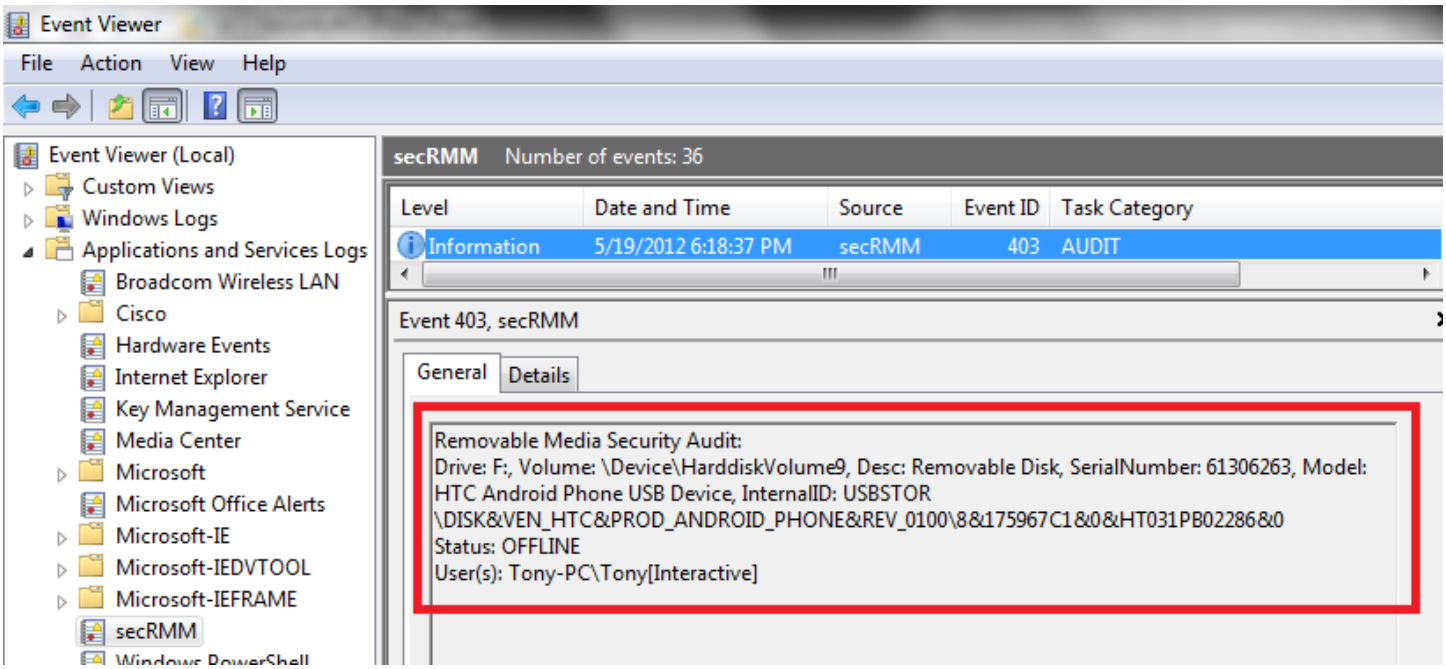


Figure 2 – secRMM offline event

Monitoring when removable media devices go online and offline is an important security feature.

Write Events

The secRMM product also logs when a file write operation to the removable media device starts[2] and completes. The 'write started' and 'write completed' secRMM events list the device, the target and source files, the program that was used and the user that performed the write operation. The secRMM 'write started' event has an event id of 401 (see Figure 4 below). The secRMM 'write completed' event has an event id of 402 (see Figure 5 below).

Details

Line 1: Removable Media Security Audit:
Line 2: Drive: F:, Volume: \Device\HarddiskVolume9, Desc: Removable Disk, SerialNumber: 61306263, Model: HTC Android Phone USB Device, InternalID: USBSTOR\DISK&VEN_HTC&PROD_ANDROID_PHONE&REV_0100\8&175967C1&0&HT031PB02286&0
Line 3: Status: WRITE COMPLETED
Line 4: Target File: H:\TakingHome\Sales for Q2 2011.xlsx
Line 5: Source File(s): C:\CorporateFinancials\Sales for Q2 2011.xlsx, Size: 8746, LastWriteTime: 02/26/2011 21:55:02
Line 6: User: Tony-PC\Tony, SID: S-1-5-21-4017941760-3181257084-2242886672-1001
Line 7: Program: "C:\Windows\system32\cmd.exe", copy "sales for q2 2011.xlsx" h:\takinghome, Current Directory: C:\CorporateFinancials, PID: 2712

Line 1	Indicates that this event is from secRMM.
Line 2	Describes the Removable Media device. Listed is the drive letter assigned by the operating system, the volume name, a brief description of the device, the manufacturer assigned serial number, the manufacturer model information and the devices internal ID.
Line 3	The status of the write operation. This value will be either WRITE STARTED or WRITE COMPLETED.
Line 4	The name of the file that is written to the Removable Media device.
Line 5	The name of the file(s) that are used as input to the write operation as well as the Size and LastWriteTime.
Line 6	The user that is performing the write operation. The Windows SID is listed in addition to the users Windows name.
Line 7	The program used to perform the write operation.

[2] The write start event is disabled when you first install secRMM. It can be enabled by setting the secRMM LogWriteDetails property which is discussed in the section "Setting the LogWriteDetails property" below. We do not recommend that you use the write start event since it is duplicate data of the write completed event (just different times).

Additional forensic data

Program information

secRMM performs additional forensic analysis when the write operation is performed by cmd.exe, explorer.exe or one of the Microsoft scripting languages (powershell, vbscript or jscript). For a cmd.exe write, secRMM will list the actual command issued (copy or move for example) and the current directory of the cmd session. This is true even if you run a 32bit cmd.exe session from a 64bit OS. For an explorer.exe write, secRMM will list the operation (i.e. copy or cut). For the scripting languages, secRMM will attempt to collect the actual source code line and script file name.

Compressed (zipped) files

For compressed/zipped files, the compressed files within the compressed file will be listed. Note that for compressed files, multiple event log messages may be generated to allow the listing of every file. If this is the case, the event log description text will list the output as "X of Y" where X will be a number from 1 to Y. Y will be the total number of event log messages that need to be generated to list all the compressed files. secRMM supports the Windows Operating System compression utility as well as the following popular 3rd party compression utilities: WinZip, 7z and WinRar.

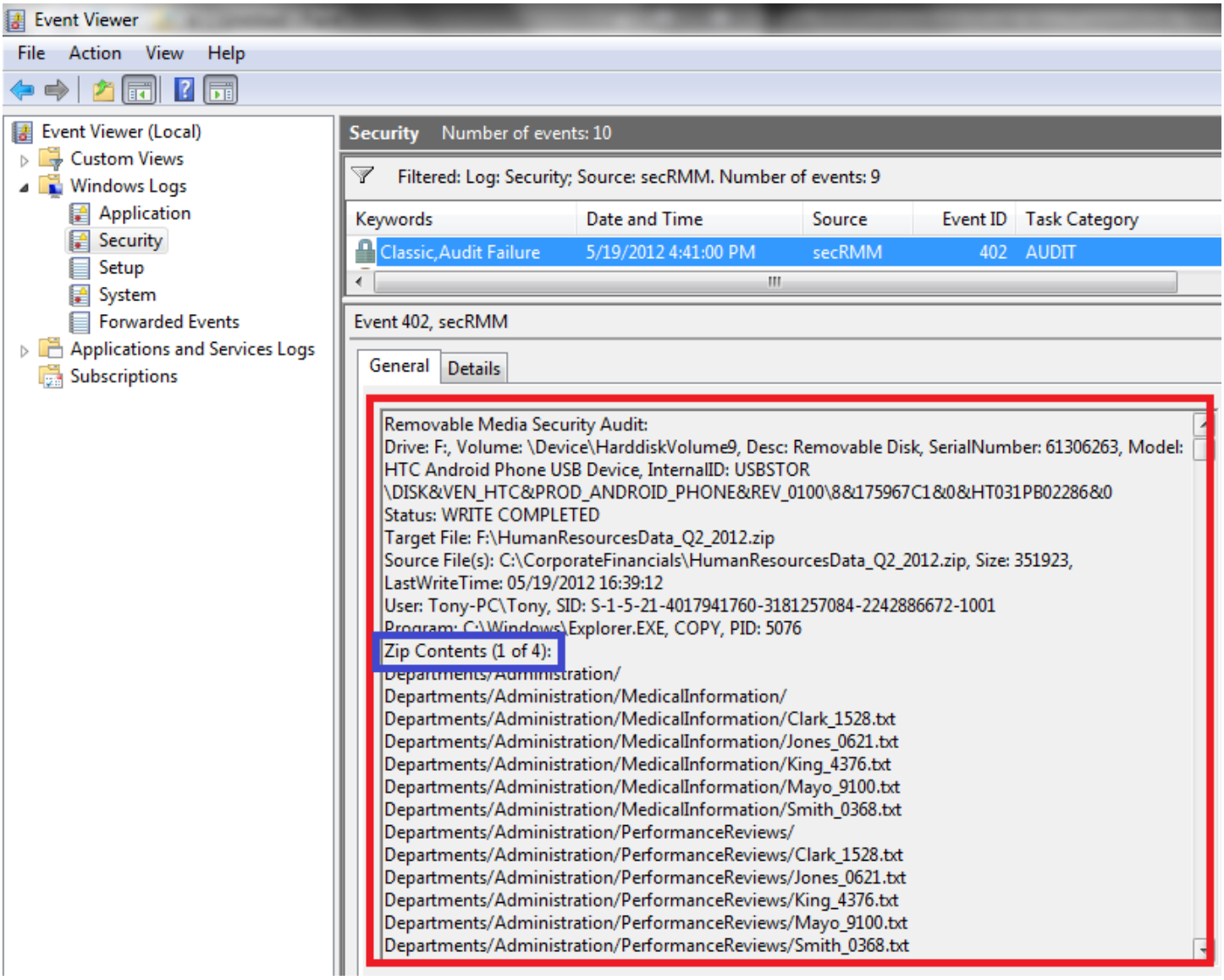


Figure 3 – Compressed File that generates multiple event log messages

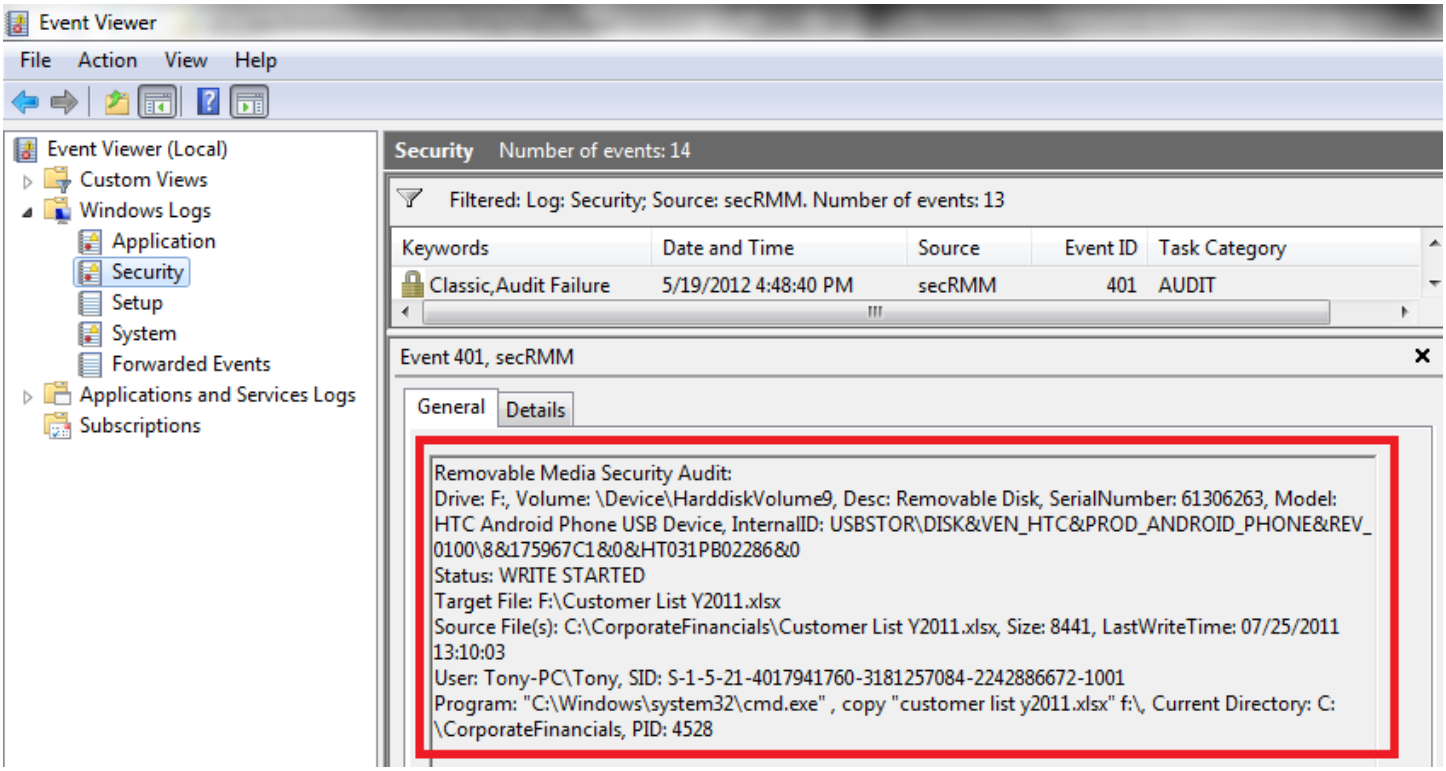


Figure 4 – secRMM write started event

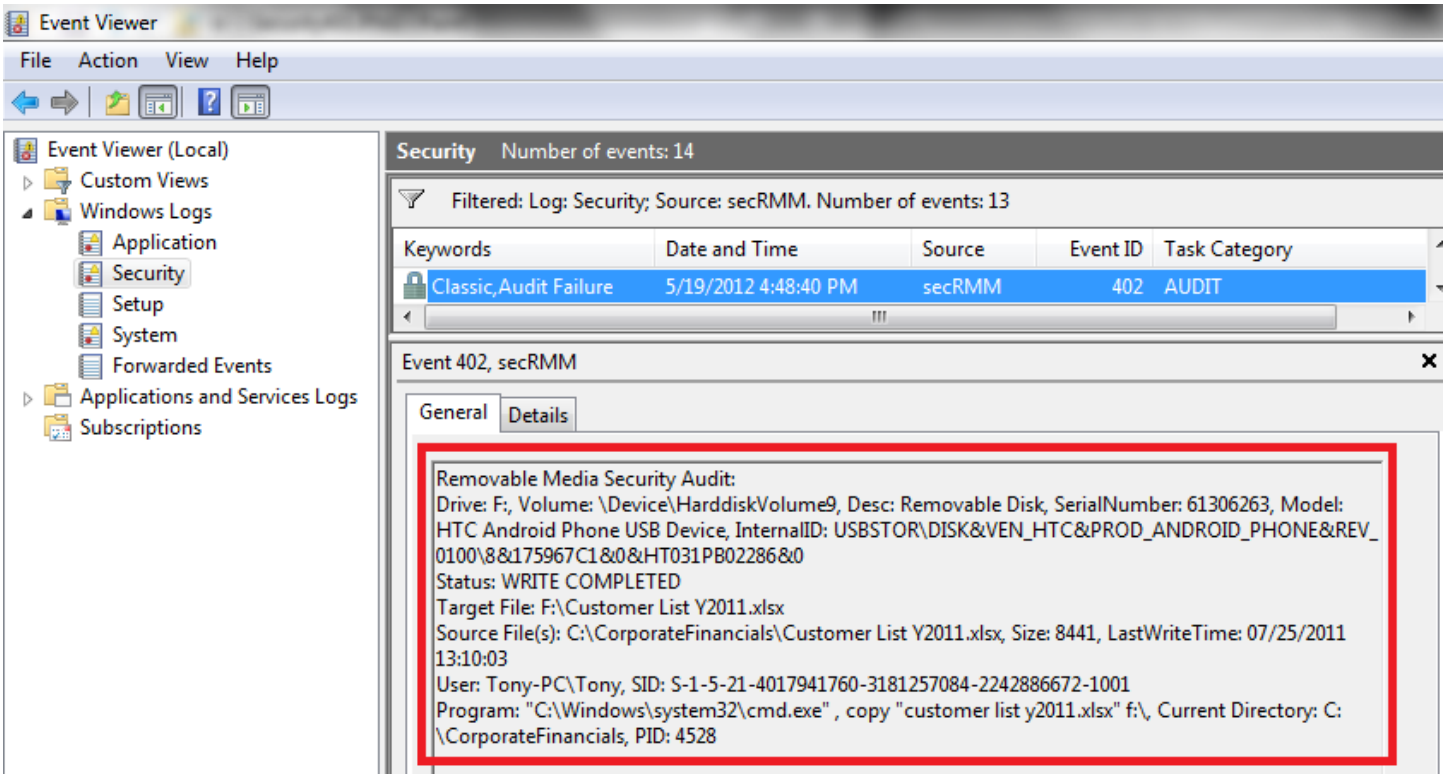


Figure 5 – secRMM write completed event

With the 4 events described above, you can be assured that your valuable data files are all accounted for!

Files from the network

The secRMM product logs when a file write operation to the removable media device comes from a network share. As you can see in Figure 6 below, the source file for this secRMM write event is coming from a networked computer. secRMM captures the source computer and the network share name in addition to the file name. Note however that the file Size and LastWriteTime are not available for source files coming over the network.

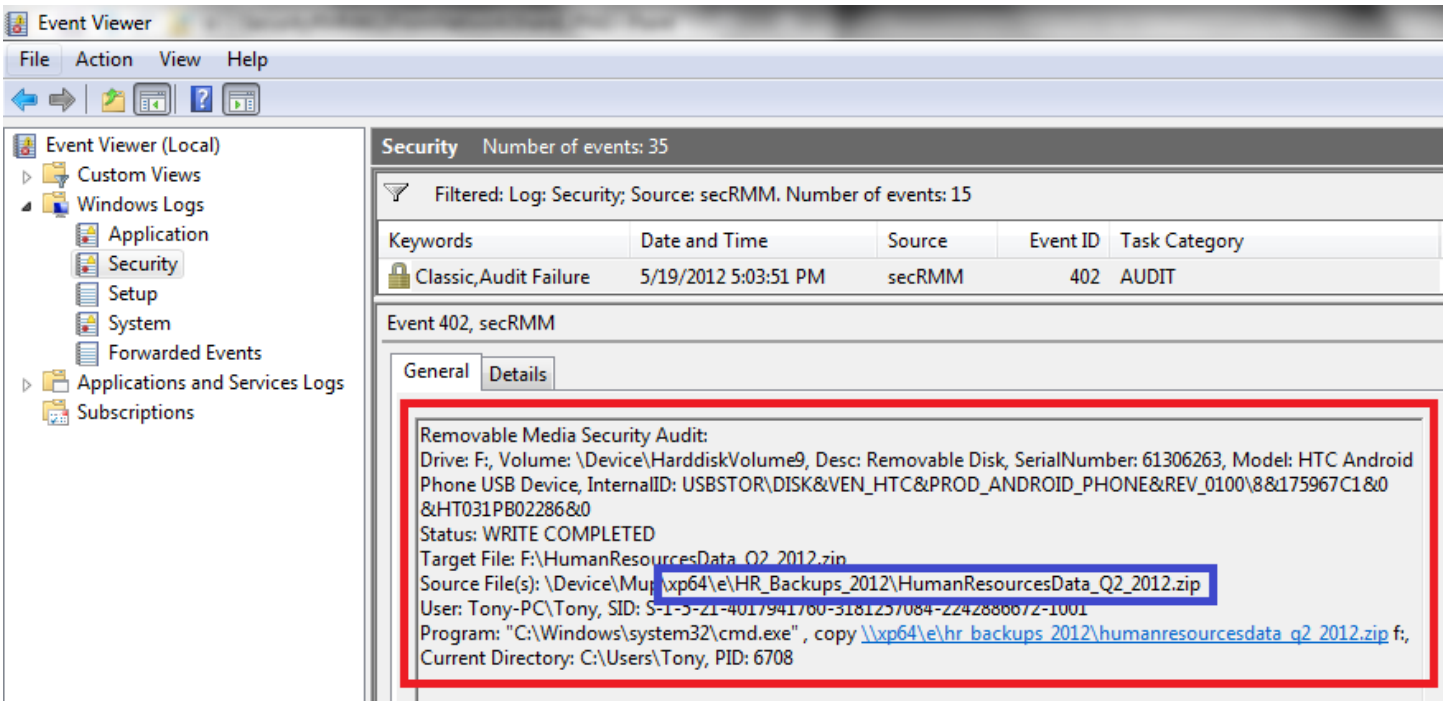


Figure 6 – secRMM copying files over the network

Use of two log files

As you can see from the screenshots so far, secRMM can log to the native Windows Security event log (see the section titled "Writing to the Windows security event log" below). However, secRMM also logs all of its events to its own Windows event log named secRMM. This allows you to view only the secRMM events (it should be pointed out here that you can also put a filter on the Security event log to achieve the same view as the secRMM log by filtering on the "event source" of secRMM). If you choose not to log secRMM events to the native Security event log, you will always have the secRMM events in the secRMM event log. A screenshot of the secRMM event log is shown below (Figure 7). The secRMM Microsoft Operations Manager Management Pack uses the secRMM event log to pick up alerts. In addition, the secRMM event log is automatically backed up and archived.

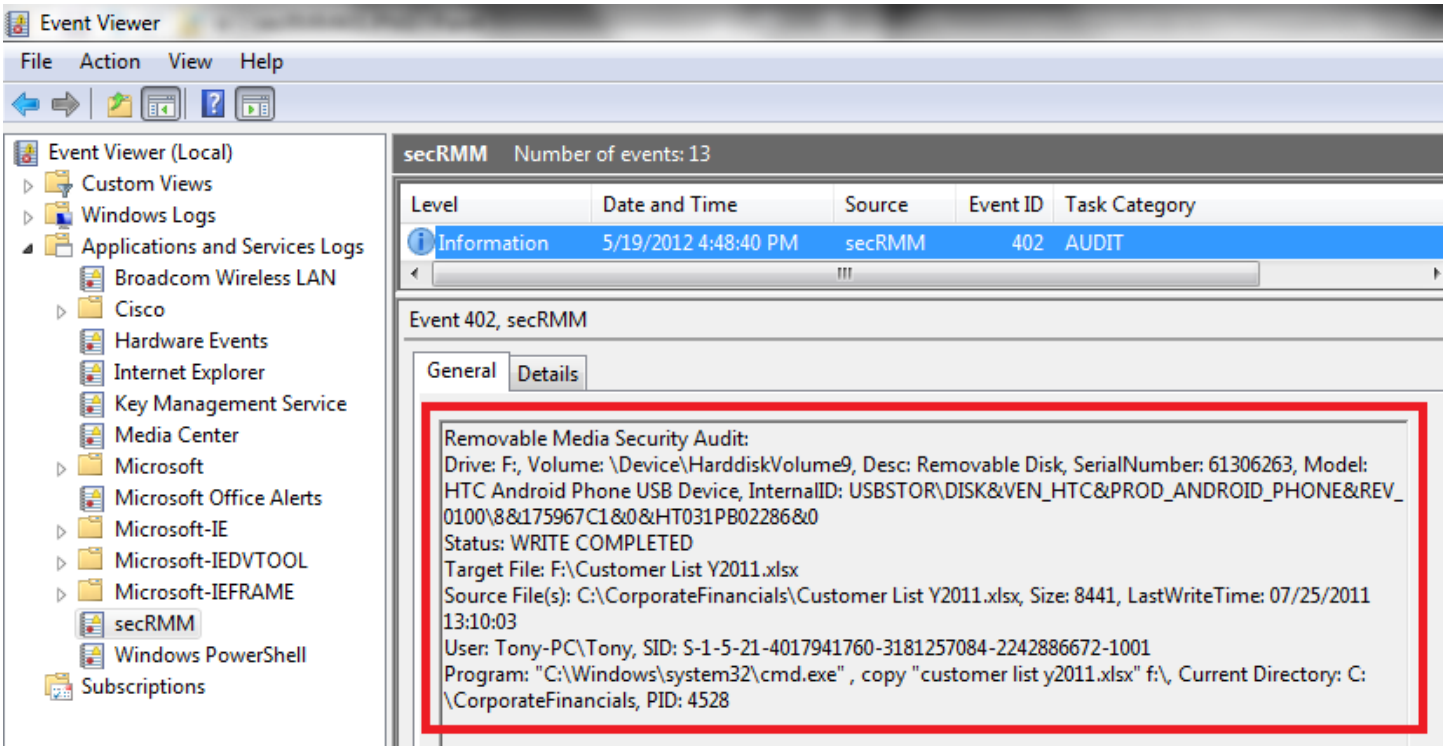


Figure 7 - The secRMM event log

The secRMM event log allows only Administrators to view and manage the secRMM event log. Your end-users will not be allowed to view the secRMM event log. If your end-users attempt to view the secRMM event log, they will get an access denied error message (see Figure 8 below).

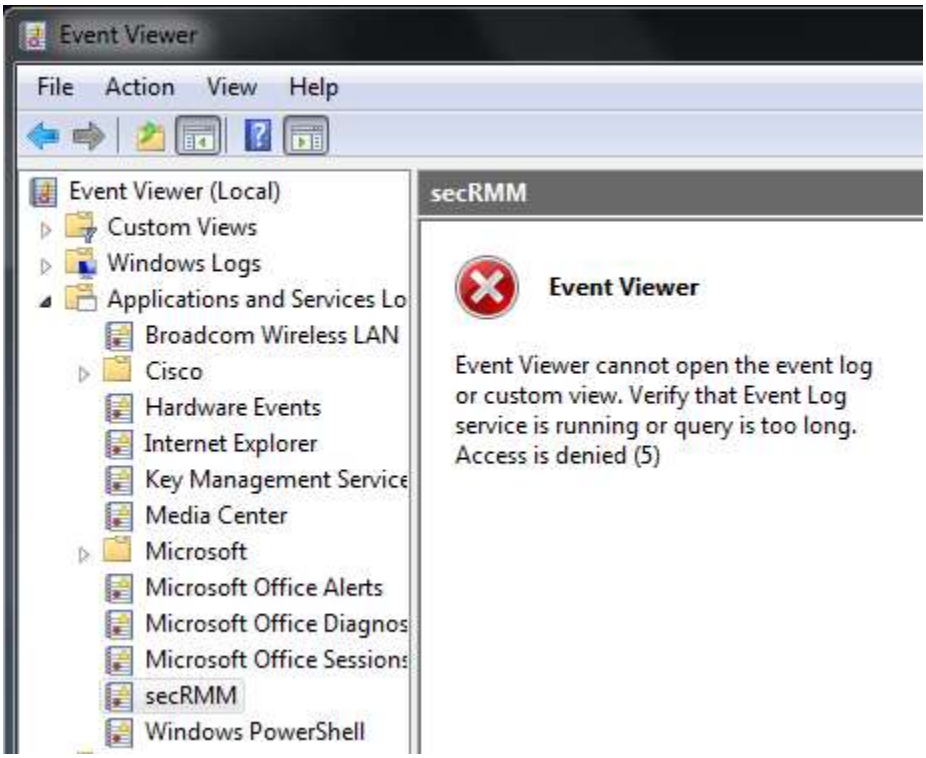


Figure 8 - End users experience when viewing the secRMM event log

Authorization mode

The secRMM product understands what device, what user, what program and what file(s) are being used when writing to removable media devices. Therefore, the secRMM product can allow you to control who and how files are written to a removable media device for each computer in your environment. There are eight secRMM properties that control authorization to removable media devices:

1. AllowBitLockerOnly
2. AllowedUsers
3. AllowedPrograms
4. AllowedSerialNumbers
5. AllowedInternalIds (Vendor Ids and/or Product Ids)
6. AllowedDirectories
7. AllowedFileExtensions
8. AllowRMSFilesOnly

A common computer term for these properties is called whitelisting. This term is equivalent to saying that you want to tell secRMM what you will "allow". Everything outside of what you will allow is called blacklisting (i.e. not allowed). When you use more than one of the whitelisting secRMM properties (listed above), they must all pass the test for the write operation to succeed. The only exception to this rule is for the device properties (AllowedSerialNumbers and AllowedInternalIds). These two rules are "ORed" together, meaning if the device being tested passes either rule, it will pass the test.

Each property (with the exceptions of AllowBitLockerOnly and AllowRMSFilesOnly which are checkbox properties) is a semi-colon separated list of the particular control (i.e. directories, file extensions, users,

programs, serial numbers and internal ids). Not setting a value for these secRMM properties puts secRMM into a monitoring only mode. This is probably an acceptable policy for most environments. However, if you do need to perform authorization functions, these are the secRMM properties to use.

The secRMM product logs 8 distinct events for authorization (corresponding to each property listed above). The 8 secRMM events are described below.

User

The secRMM product logs when a user is trying to write to a removable media device but is not in the "Allowed Users" list. The secRMM event for this "unauthorized user" event has an event id of 500 (see Figure 9).

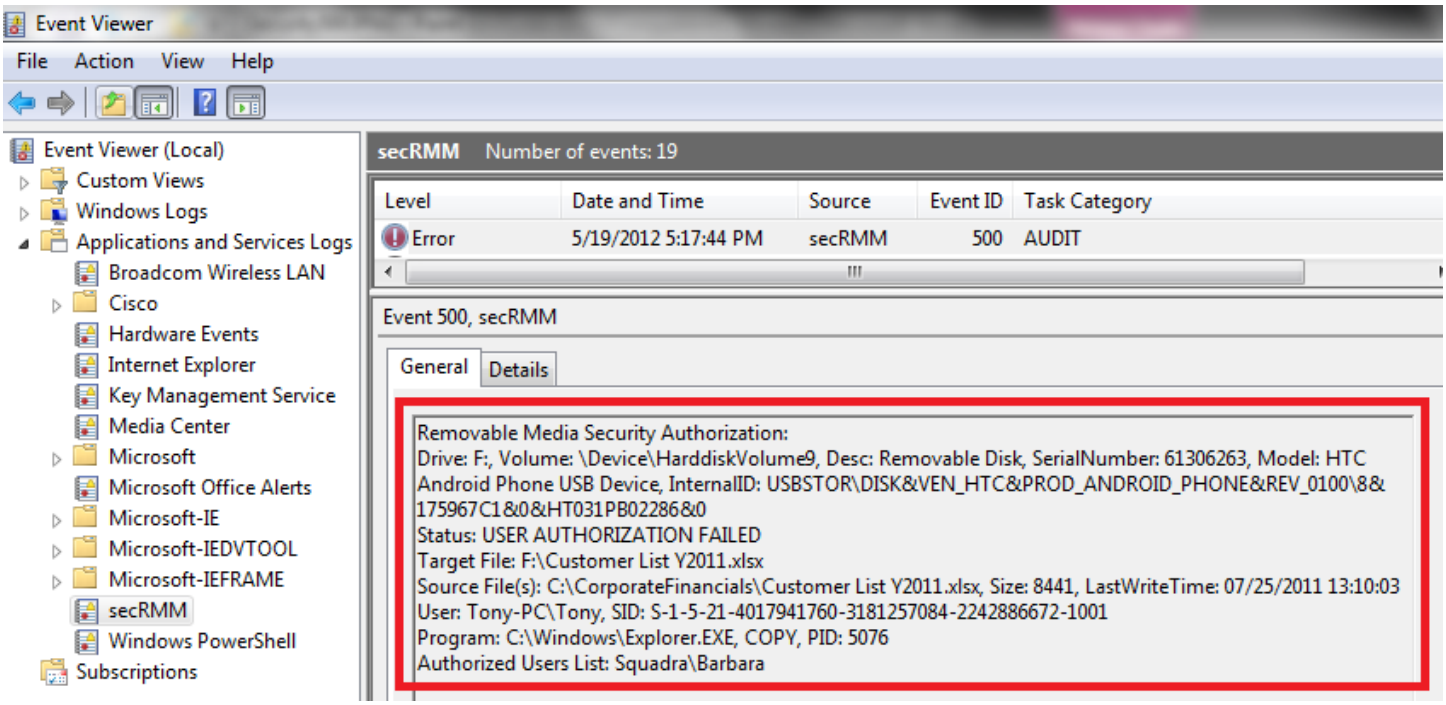


Figure 9 – secRMM User Authorization failed event

Program

The secRMM product logs when a specific program is being used to write to the removable media device but the program is not in the "Allowed Programs" list. The secRMM event for this "unauthorized program" has an event id of 501 (see Figure 10).

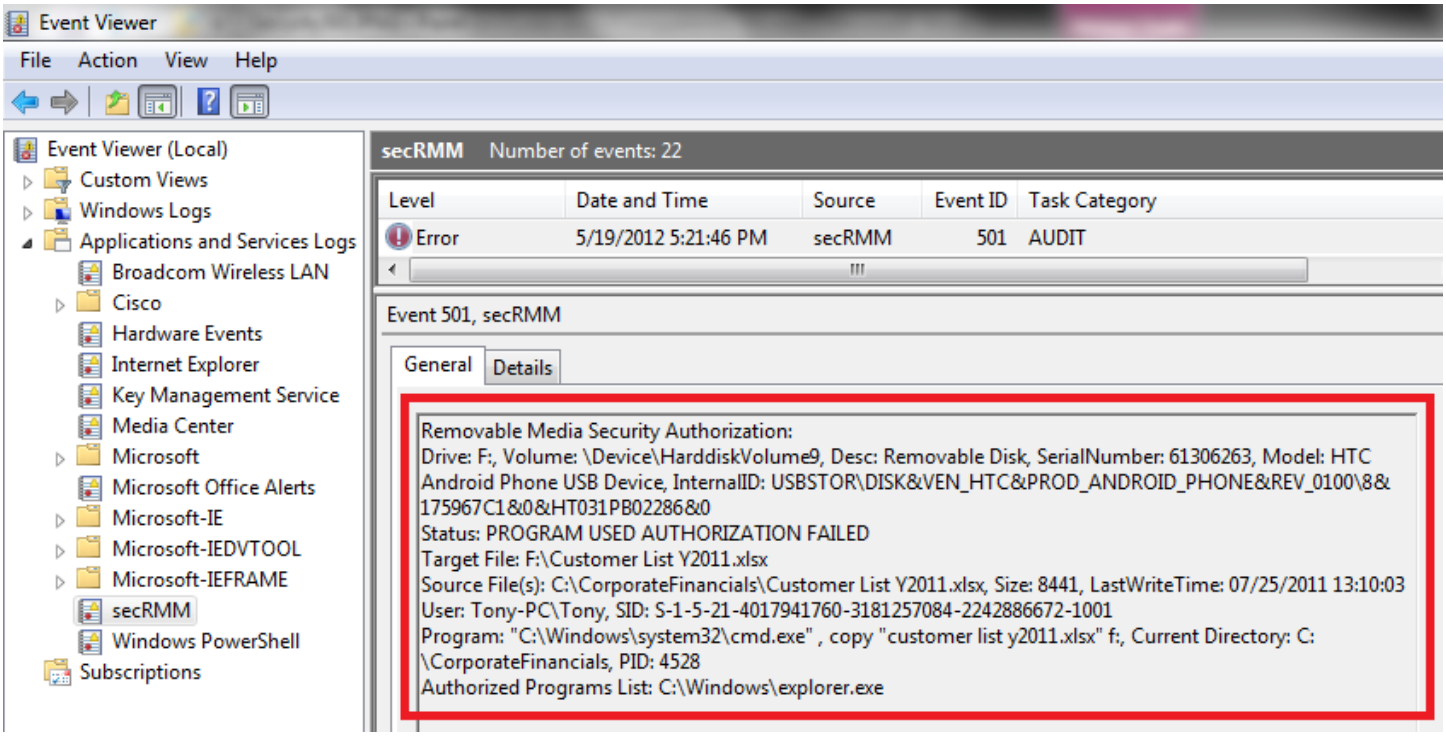


Figure 10 - secRMM Program Authorization failed event

Serial number

The secRMM product logs when a removable media device serial number being used to write is not in the "Allowed Serial Numbers" list. The secRMM event for this "unauthorized serial number" has an event id of 502 (see Figure 11).

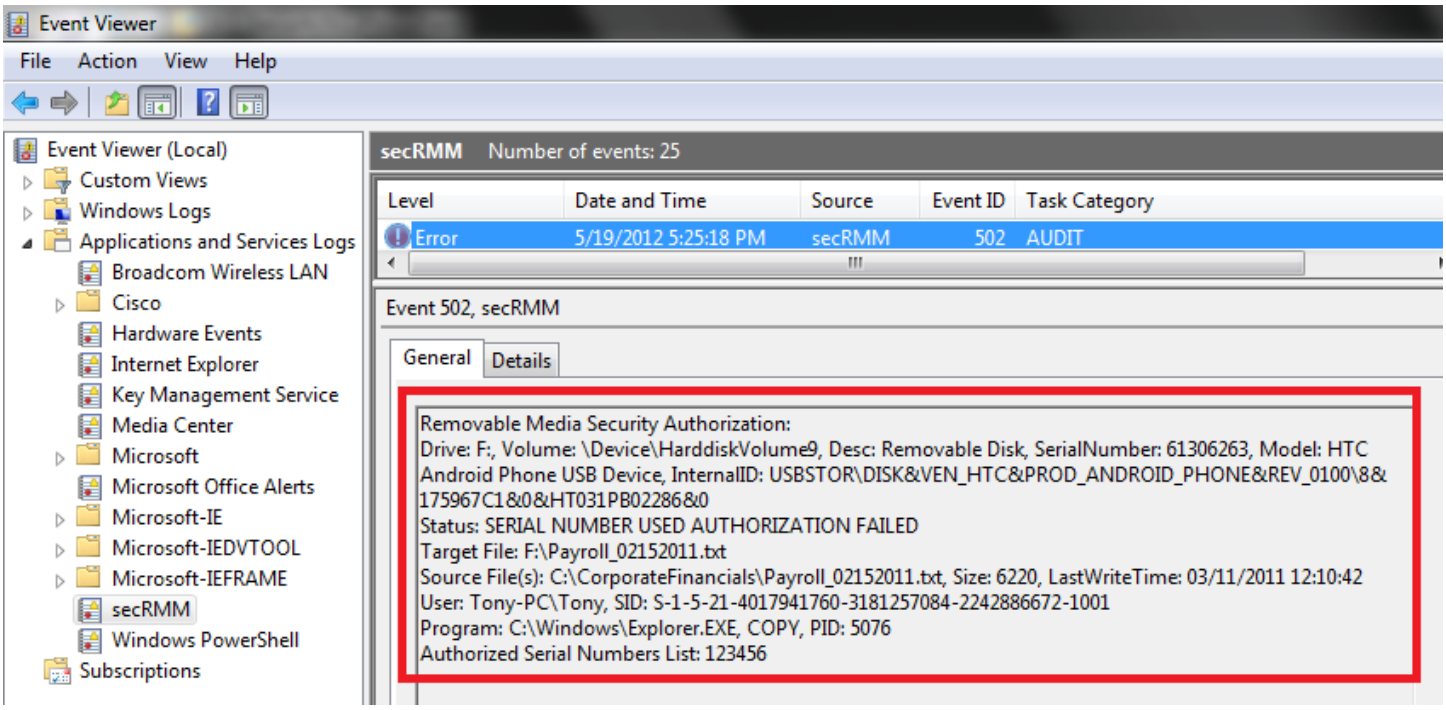


Figure 11 - secRMM Serial Number Authorization failed event

Internal Ids

The secRMM product logs when a removable media device with an Internal Id being used to write is not in the "Allowed Internal Ids" list. The secRMM event for this "unauthorized Internal Id" has an event id of 506 (see Figure 12).

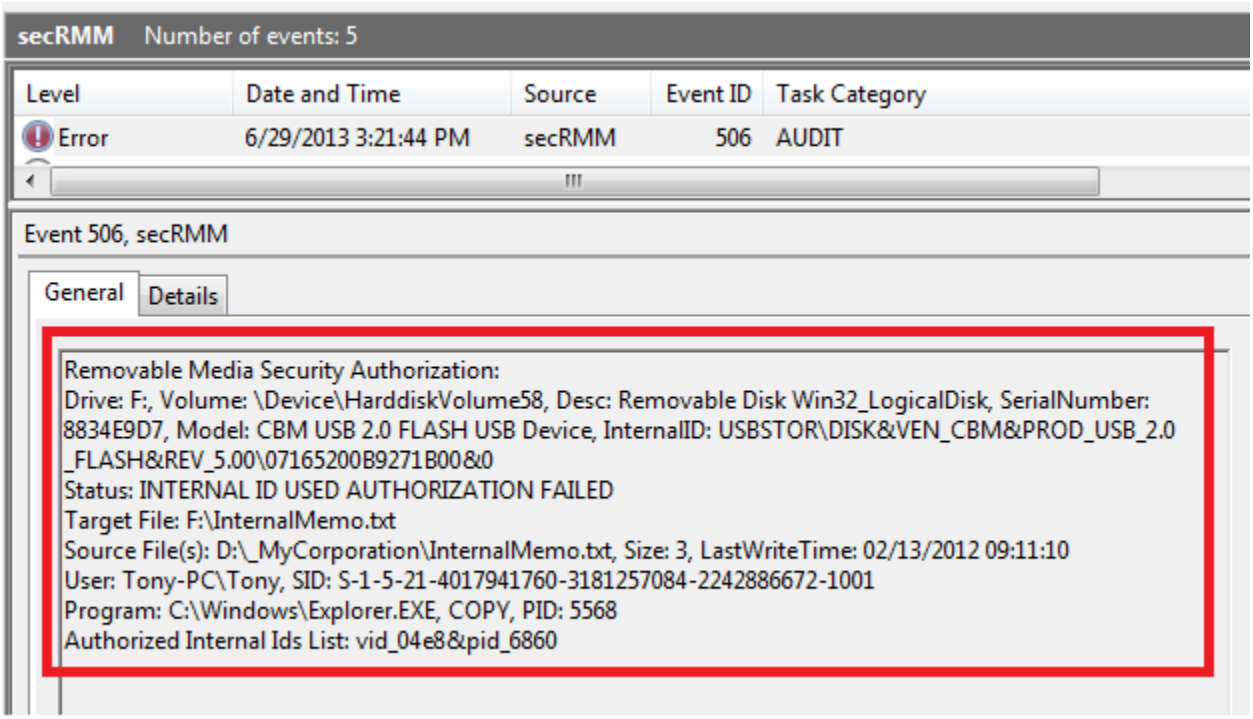


Figure 12 - secRMM Internal Id Authorization failed event

Directory

The secRMM product logs when a user tries to copy files from a directory that is not in the "Allowed Directories" list. The secRMM event for this "unauthorized source directory" has an event id of 504 (see Figure 13).

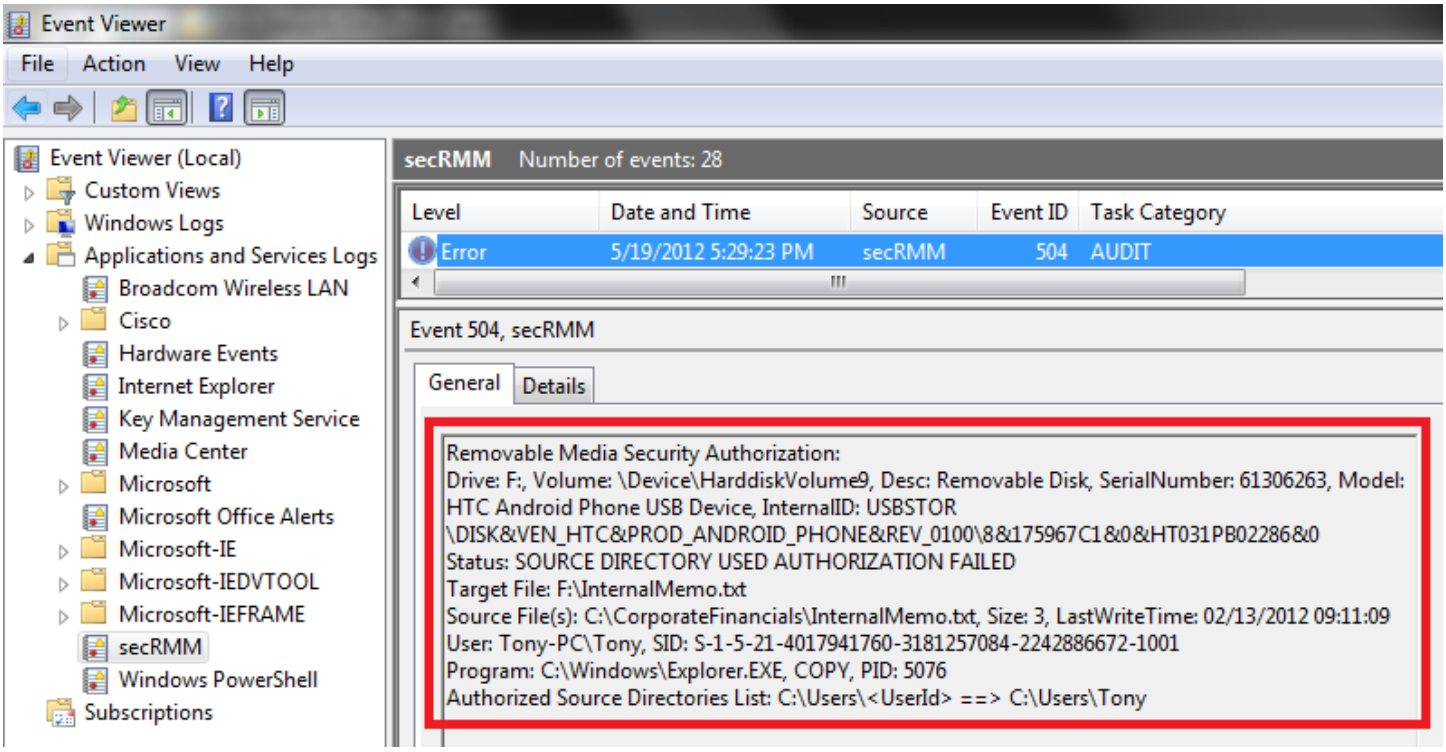


Figure 13 - secRMM Source Directory Authorization failed event

File Extension

The secRMM product logs when a user tries to copy file(s) that have an extension that is not in the "Allowed File Extensions" list. The secRMM event for this "unauthorized file extension" has an event id of 505 (see Figure 14).

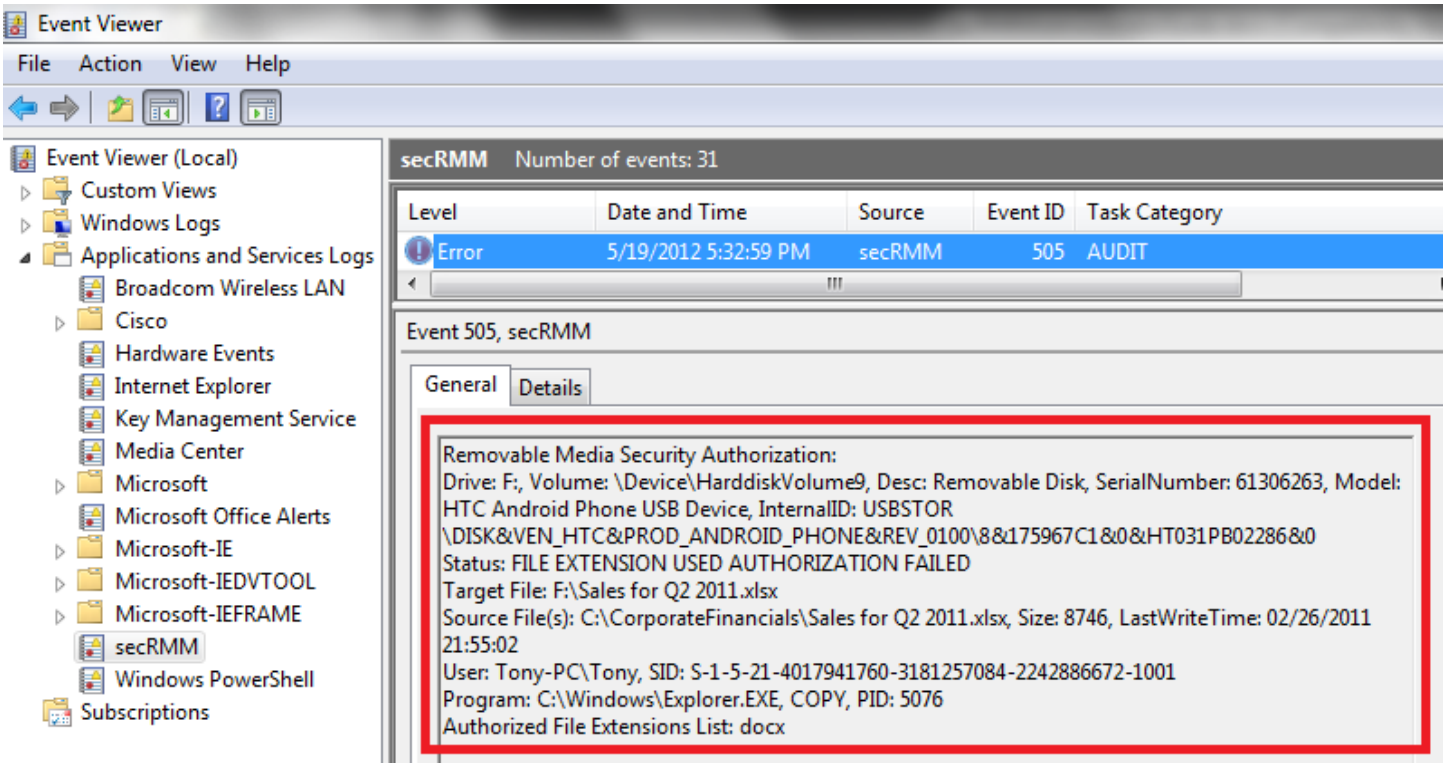


Figure 14 - secRMM File Extension Authorization failed event

BitLocker Only

The secRMM product logs when a user tries to copy file(s) to a device that is not BitLocker enabled when the "Allow BitLocker only" rule is enabled (checked). The secRMM event for this "unauthorized device" has an event id of 513 (see Figure 15).

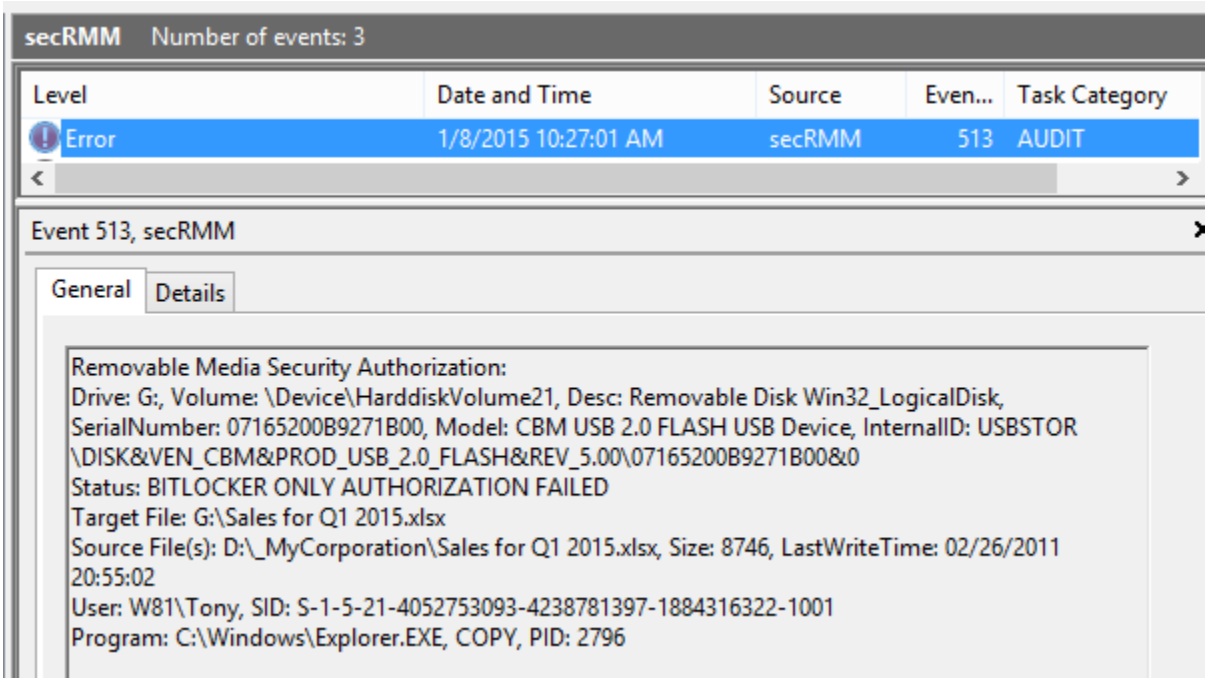


Figure 15 - secRMM Allow BitLocker only failed event

Allow RMS Files Only

The secRMM product logs when a user tries to copy file(s) that are not protected by Microsoft Rights Management Services (RMS) to a removable storage device when the "Allow RMS Files only" rule is enabled (checked). The secRMM event for this "unauthorized file copy" has an event id of 515 (see Figure 15).

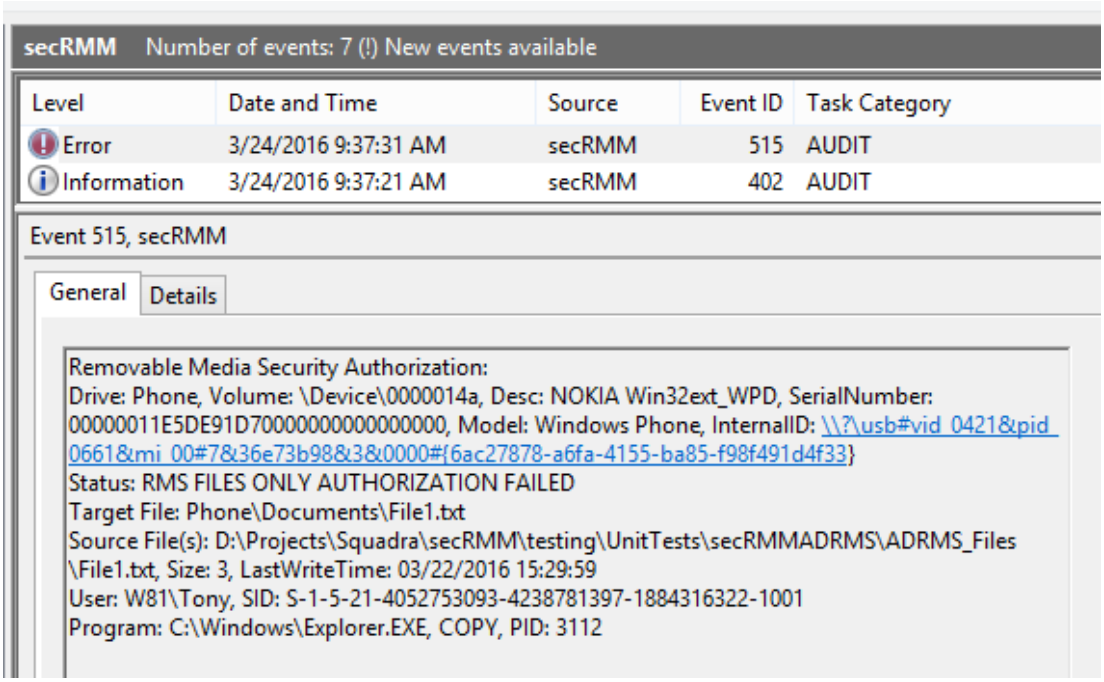


Figure 16 - secRMM Allow RMS Files Only

End-user experience on authorization failures

When one of the authorization failure events occur, the end user will see this as an access denied (see Figure 17 and Figure 18 below).

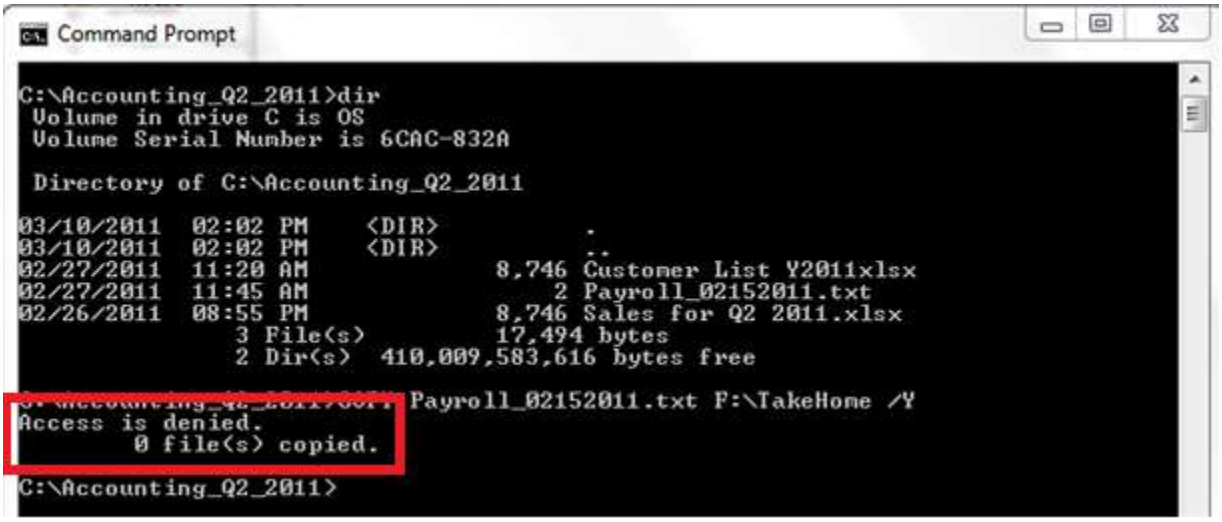


Figure 17 - Users view of an authorization failure in a cmd session

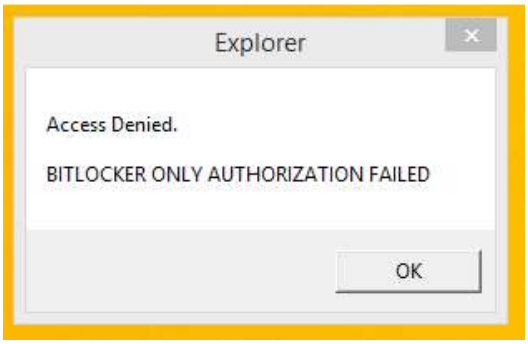


Figure 18 - Users view of an authorization failure from Windows Explorer

To understand how to enable and disable each secRMM authorization property, please see the section below titled "Enabling Authorization".

Monitoring secRMM Administration changes

When an Administrator changes one of the secRMM properties, secRMM monitors the change event. The secRMM event id for administration events is 700 (see Figure 19). Monitoring who is authorizing specific use of Removable Media devices is just as important as monitoring who is using the Removable Media devices!

Additionally, when a secRMM user policy is created, secRMM will generate an event id 701. The 701 event tells you the administrator who created the user policy and what userid the policy is created for.

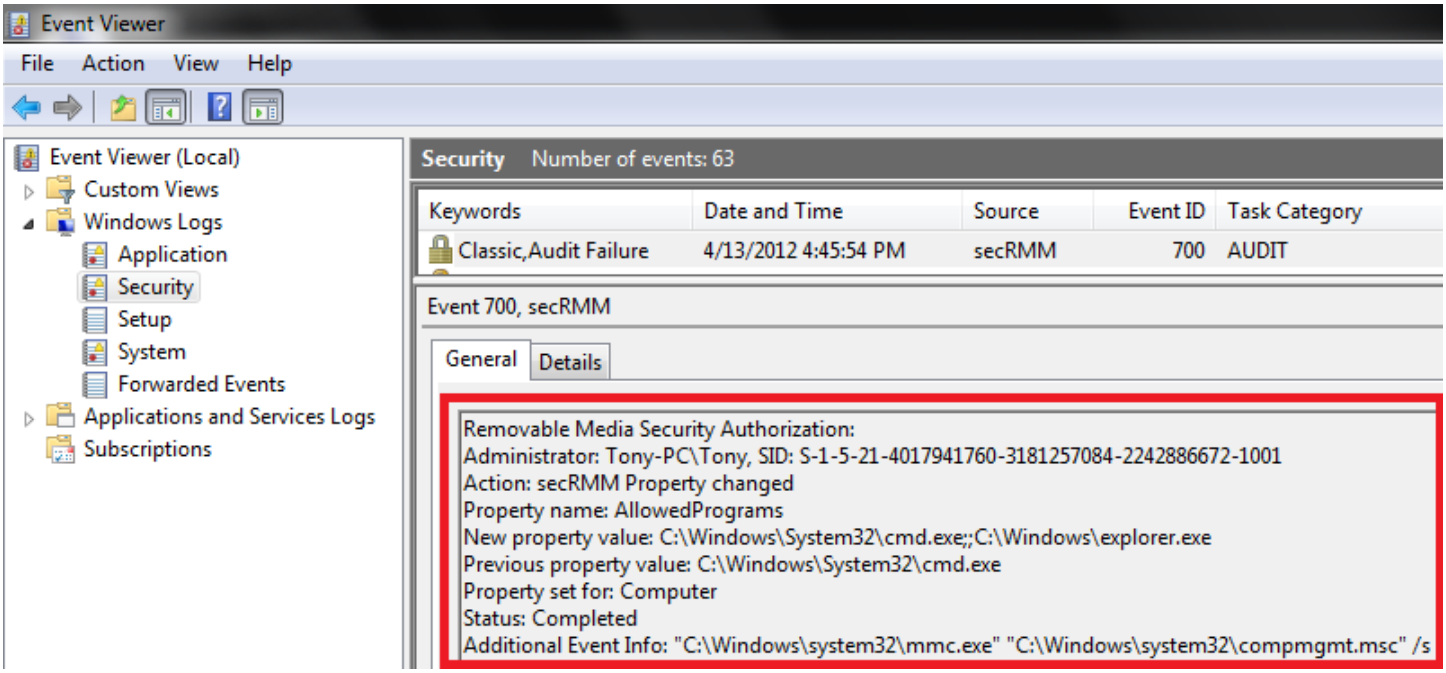


Figure 19 - secRMM authorization monitoring

Lockdown mode

Putting secRMM in lockdown mode will prevent any write activities to Removable Media devices. You can set secRMM into lockdown mode at installation time. secRMM lockdown mode is really just a special case of authorization mode in that you only need to set one of the secRMM authorization properties to an invalid value (using the AllowedSerialNumbers is probably the best choice). Please read the section below titled "Preventing write activity to Removable Media – Lockdown mode" for specifics on using scripts to put a machine into secRMM lockdown mode.

Eject mode

Eject mode runs as soon as the device is connected to the Windows computer. Eject mode checks the device serial number, the device internal id and the logged in users against the secRMM authorization properties of the same name. If there is a mismatch, secRMM ejects the device so that to the end-user, the device appears to have never been mounted by the Windows operating system.

****

You have reached the end of the "Introduction" section of this manual. The next two major sections are "Installation" and "Configuration". These sections are intended for the IT administrators who are responsible for installing and configuring secRMM.

Installation

Overview

The secRMM installation is a standard Windows installation program. It uses the following Microsoft installer versions for the different Windows Operating System versions:

> Windows Installer 5.0 on Windows Server 2008 (R2), Windows 2012 (R2), Windows 7, Windows 8.1, Windows 10
>
> Windows Installer 4.0 or Windows Installer 4.5 on Windows Server 2008 or Windows Vista
>
> Windows Installer on Windows Server 2003, Windows XP, and Windows 2000

If you keep current with Microsoft Updates, you will already have these versions on your systems.

System Requirements

The secRMM installation requires that you perform the installation while logged in as an Administrator. If you attempt to perform the installation and are not an Administrator, the final step of the installation process will prompt you to login as an Administrator before it will actually perform the installation.

The secRMM product was designed to run on Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008 and Windows Server 2012 and Windows 10. The secRMM product provides a 64bit and 32bit version. Any CPU configuration is supported. The secRMM product requires the Windows Management Instrumentation (WMI) service and Microsoft .Net Framework version 4.0.

Interactive Installation

You can simply double click the secRMMInstallx64.msi (for 64bit) or secRMMInstallx86.msi (for 32bit) file from Windows Explorer to perform an interactive installation. By default, secRMM will install to the boot drive under the "Program Files" directory. However, you are able to override the default directory during the installation.

License Agreement

The End-User License Agreement is presented during the installation process (see Figure 20). You can print the End-User License Agreement if required.

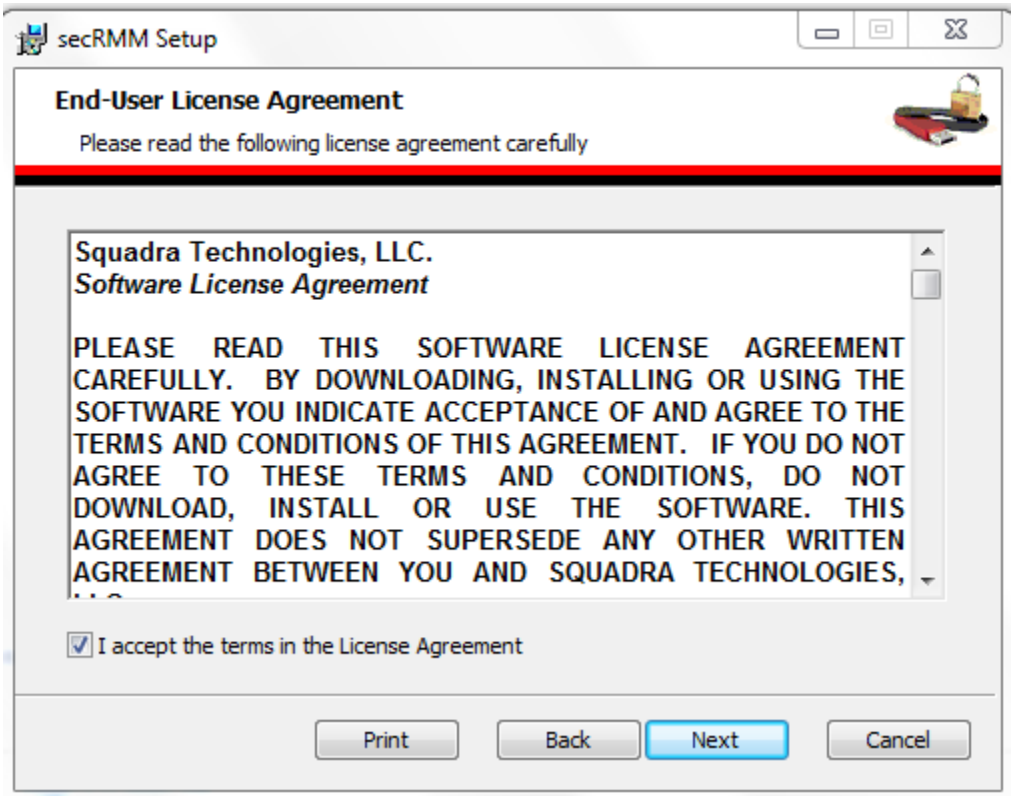


Figure 20 - secRMM License Agreement

Custom Installation

Choosing Lockdown Mode at installation time

By default, secRMM installs in monitoring mode. This means write activity to Removable Media is still permitted. Of course all the write activity will be recorded to the event log(s) by secRMM.

You may be in an environment where you want to disable Removable Media write activity and only allow Removable Media write activity using secRMM authorization properties (i.e. specifically give user(s) and/or program(s) and/or serial numbers permission). This secRMM mode is called Lockdown. During installation, you can select secRMM Lockdown mode (see Figure 21 below).

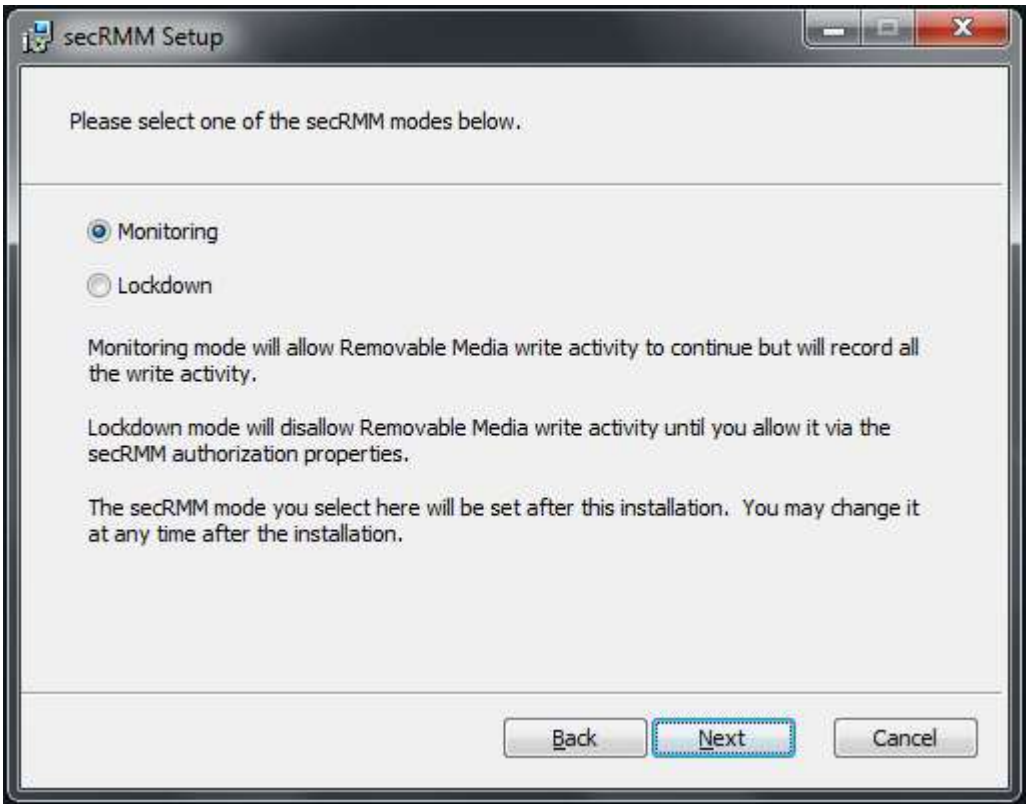


Figure 21 - Selecting the secRMM mode at installation time

Choosing to use SafeCopy at installation time

SafeCopy is an end-user GUI application that ships with secRMM. SafeCopy works in conjunction with secRMM to provide a higher level of security and monitoring of removable media write activity. The SafeCopy user interface mimics the standard Windows explorer program but only allows writing to removable media. SafeCopy also implements a "two man" policy (i.e. at least 2 people must be involved for the removable media write operation to occur). The two man policy concept is a common operating procedure in many critical military situations. The SafeCopy Approval program can be run remotely and uses a TCP/IP connection to communicate with the SafeCopy program. Therefore, an inbound firewall rule is required. You can optionally specify to have the secRMM installation create the firewall rule. If you choose to have the secRMM installation program create the inbound firewall rule, it will be named "secRMMSafeCopy". You can also manually create the firewall rule if you choose not to have the secRMM installation create it. Details on how to create the firewall rule manually are in the section titled "Firewall rule for secRMM SafeCopy Approver" (below).

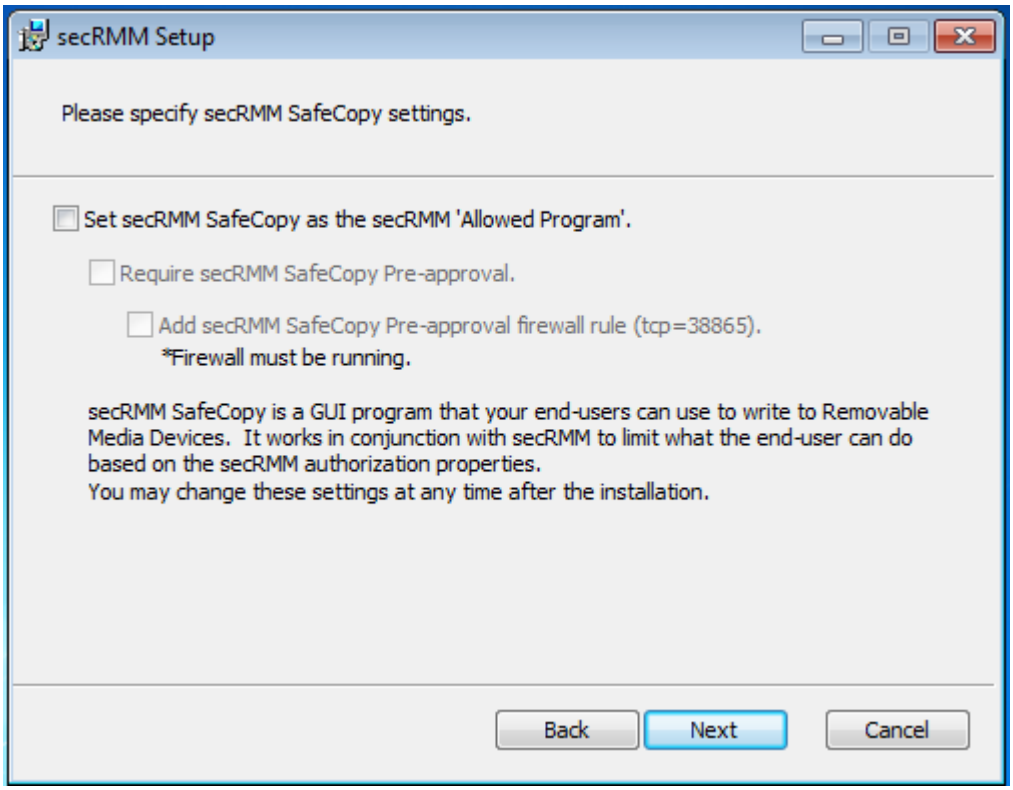


Figure 22 - Selecting the secRMM SafeCopy properties at installation time

Silent Installation

From a cmd window that is running in Administrator mode, type one of the following lines based on whether you are installing on a 64bit OS or a 32bit OS:
msiexec /quiet /i secRMMInstallx64.msi
msiexec /quiet /i secRMMInstallx86.msi

You can customize the silent installation by specifying different properties (variables) on the command line. secRMM supports the following installation properties:

Property Name	Value	Purpose
INSTALLLOCATION	Hard drive path	Specifies the secRMM installation directory
SECRMMLOCKDOWNMODE	ON	Specifies that secRMM is installed in lockdown mode
SAFECOPYISALLOWEDPROGRAMUI	ON	Specifies that secRMM is installed with SafeCopy as the only program in the secRMM AllowedPrograms property
REQUIRESAFECOPYPREAPPROVALUI	ON	Specifies that SafeCopy requires pre-approval (i.e. the two-man policy scheme)

ADDSAFECOPYFIREWALLRULEUI	ON	Create the SafeCopy pre-approval firewall rule
ARPSYSTEMCOMPONENT	1	Specifies to not list secRMM as an installed program in the Add/Remove programs list
PREVENTSTARTMENUPINNING	1	Specifies to not pin the secRMM SafeCopy GUI program to the Windows Start Menu (pinning is the default)
PREVENTALLPROGRAMSPINNING	1	Specifies to not pin the secRMM SafeCopy GUI program to the Windows "All Programs" Menu (pinning is the default). Note that if you set this property, it will force property PREVENTSTARTMENUPINNING to 1 as well.

The subsections below explain each of these secRMM installation properties.

Overriding the default Installation directory

From a cmd window that is running in Administrator mode, type one of the following lines based on whether you are installing on a 64bit OS or a 32bit OS. The example below assumes you want secRMM to install to the D drive under the folder named Apps.
msiexec /quiet /i secRMMInstallx64.msi INSTALLLOCATION=D:\Apps\secRMM
msiexec /quiet /i secRMMInstallx86.msi INSTALLLOCATION=D:\Apps\secRMM

Specifying secRMM Lockdown mode

From a cmd window that is running in Administrator mode, type one of the following lines based on whether you are installing on a 64bit OS or a 32bit OS.
msiexec /quiet /i secRMMInstallx64.msi SECRMMLOCKDOWNMODE=ON
msiexec /quiet /i secRMMInstallx86.msi SECRMMLOCKDOWNMODE=ON

Specifying SafeCopy as the secRMM Allowed Program

From a cmd window that is running in Administrator mode, type one of the following lines based on whether you are installing on a 64bit OS or a 32bit OS.
msiexec /quiet /i secRMMInstallx64.msi SAFECOPYISALLOWEDPROGRAMUI=ON
msiexec /quiet /i secRMMInstallx86.msi SAFECOPYISALLOWEDPROGRAMUI=ON

Specifying SafeCopy requires preapproval

From a cmd window that is running in Administrator mode, type one of the following lines based on whether you are installing on a 64bit OS or a 32bit OS.
msiexec /quiet /i secRMMInstallx64.msi REQUIRESAFECOPYPREAPPROVALUI=ON
msiexec /quiet /i secRMMInstallx86.msi REQUIRESAFECOPYPREAPPROVALUI=ON

Specifying SafeCopy preapproval firewall rule

From a cmd window that is running in Administrator mode, type one of the following lines based on whether you are installing on a 64bit OS or a 32bit OS.
msiexec /quiet /i secRMMInstallx64.msi ADDSAFECOPYFIREWALLRULEUI=ON
msiexec /quiet /i secRMMInstallx86.msi ADDSAFECOPYFIREWALLRULEUI=ON

Don't list secRMM in the Add/Remove Programs list

You can prevent secRMM from being listed in the Add/Remove Programs list by setting the install variable ARPSYSTEMCOMPONENT=1. While it is not really necessary to do this since you must be an Administrator to install and uninstall secRMM, some environments have requested this feature to hide the product from even the Administrators.

msiexec /i secRMMInstallx64.msi ARPSYSTEMCOMPONENT=1
msiexec /i secRMMInstallx86.msi ARPSYSTEMCOMPONENT=1

Don't pin SafeCopy to the Windows Start Menu

You can prevent secRMM from pinning the SafeCopy program to the Windows Start Menu by setting the install variable PREVENTSTARTMENUPINNING=1.

msiexec /i secRMMInstallx64.msi PREVENTSTARTMENUPINNING=1
msiexec /i secRMMInstallx86.msi PREVENTSTARTMENUPINNING=1

Don't pin SafeCopy to the Windows All Programs Menu

You can prevent secRMM from pinning the SafeCopy program to the Windows All Programs Menu by setting the install variable PREVENTALLPROGRAMSPINNING.

msiexec /i secRMMInstallx64.msi PREVENTALLPROGRAMSPINNING=1
msiexec /i secRMMInstallx86.msi PREVENTALLPROGRAMSPINNING=1

Large Scale Deployment

Deploying any software to many computer systems is best accomplished by a software product specializing in software deployment. Products of this nature typically have an agent on each computer and servers move the installation to these agents. In Windows environments, the most popular product by far is Microsoft's System Center Configuration Manager (formerly known as SMS, now known as SCCM). You can also deploy secRMM using Microsoft Active Directory Group Policy Objects (AD GPO).

Both the AD GPO and SCCM deployments are described in separate documents found on the Squadra Technologies web site. They are named **Active Directory Installation Guide** and **SCCM Installation Guide**. These documents provides a screen shot of each step required in the process. You should download and use either one of these documents for a large scale deployment.

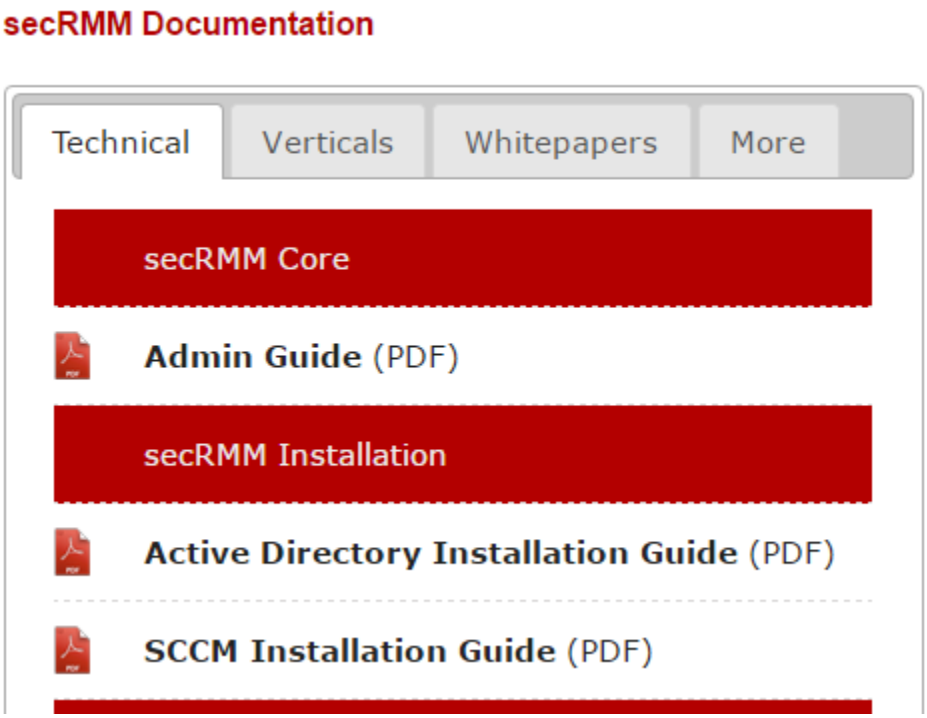


Figure 23 - Large scale deployment install guides on web site

Upgrades and Uninstallation

There are no special conditions to upgrade or uninstall secRMM other than you may be required to reboot the computer in order for the upgrade to take effect.

Configuration

Overview

The secRMM product does not require any configuration after it is first installed. After installation, secRMM will monitor all removable media write operations. The secRMM product will write all of its events into the Windows event log file named secRMM. The sections below describe the configuration options available for secRMM.

1. You can configure your environment to have secRMM write the secRMM events to the Windows security event log as well. To do this, follow the subsection titled "Writing to the Windows security event log" in the "secRMM properties" section below.
2. You can enable the authorization component of secRMM by enabling one or more of the following secRMM properties:
    a. AllowBitLockerOnly (also supports check at mount time)
    b. AllowedDirectories
    c. AllowedFileExtensions

   d. AllowedInternalIds (also supports check at mount time)
   e. AllowedPrograms
   f. AllowedSerialNumber (also supports check at mount time)
   g. AllowedUsers (also supports check at mount time)
   h. AllowRMSFilesOnly

   To enable the authorization component of secRMM, follow the subsection titled "Enabling Authorization" in the "secRMM properties" section below.
3. You can configure secRMM to treat CD-ROM, DVD and Floppy disks as removable media. To do this, follow the subsection titled "CDROM, DVD, Floppy drives" in the "secRMM properties" section below.
4. You can enable secRMM so that if the source file of a write operation cannot be determined, the write operation will fail. To do this, follow the subsection titled "Setting the FailWriteIfSourceFileUnknown property" in the "secRMM properties" section below.
5. You can enable secRMM so that a write operation will record the start event as well as the completion event. To do this, follow the subsection titled "Setting the LogWriteDetails property" in the "secRMM properties" section below.
6. You can configure secRMM to generate SNMP traps (or informs) for SNMP versions 1, 2 and/or 3. There is a section below titled SNMP.

In general, any secRMM configuration that needs to be performed is accomplished by setting secRMM properties (overviewed in the above paragraph and detailed in the sections below). To set secRMM properties, you can use:

1. The Computer Management MMC
2. A script (powershell, vbscript, jscript or cmd)
3. Active Directory Group Policy Objects (GPO)
4. Microsoft System Center Configuration Manager (SCCM)
5. Microsoft System Center Operations Manager (SCOM)

The subsections below provide the details on configuring secRMM.

Writing to the Windows security event log

The Windows Operating System requires that you enable the local security policy called "object access" so that software other than the operating system can write to the security event log. To enable secRMM to be able to write the secRMM events into the Windows security event log, you must enable the local security policy called "object access". To enable the local security policy called "object access" on the computer where secRMM is installed, please follow the steps below:

1. From the Administrative Tools menu item, select "Local Security Policy". If the Administrative Tools menu item is not on the main start menu, go into the "Control Panel" to access it.

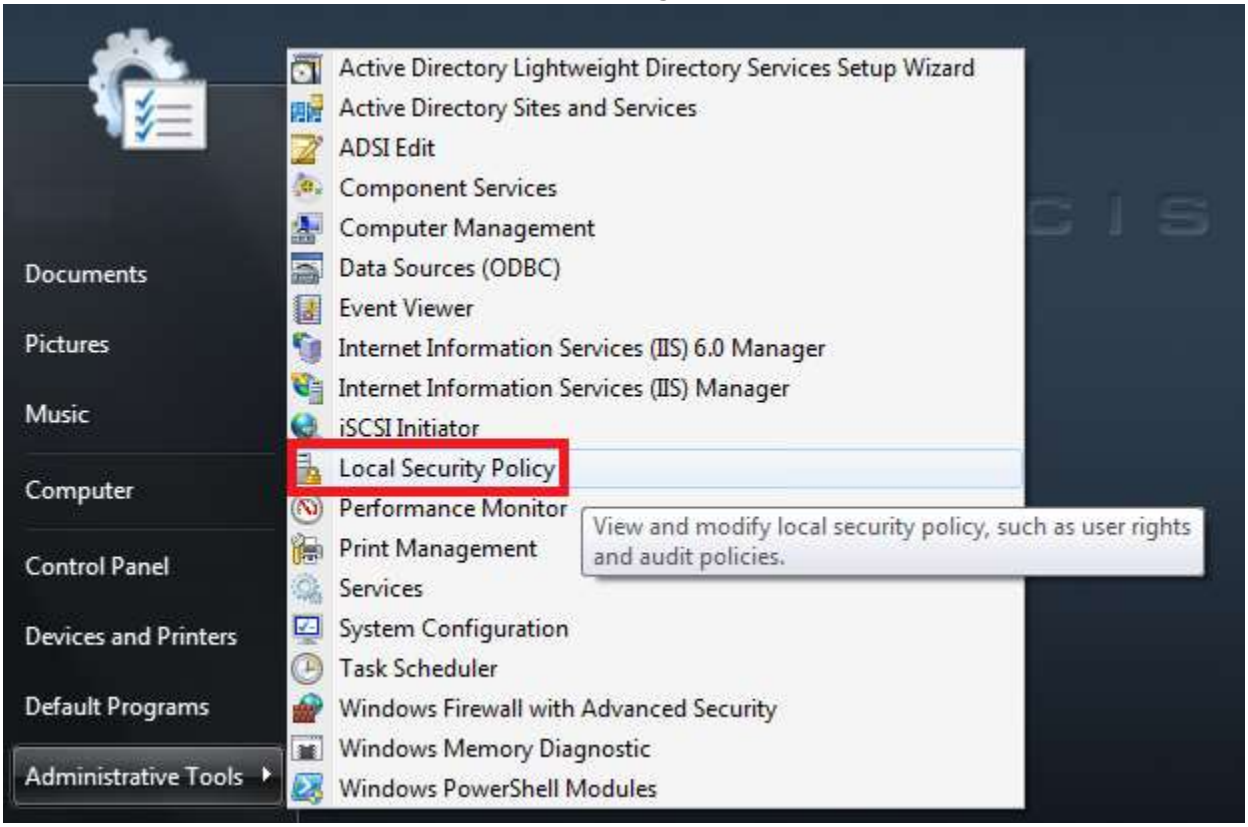


Figure 24 - Invoking the Local Security Policy

2. In the "Local Security Policy" window, expand the tree view on the left as: Security Settings=>Local Policies=>Audit Policy.
3. In the details pane on the right, double click "Audit object access"

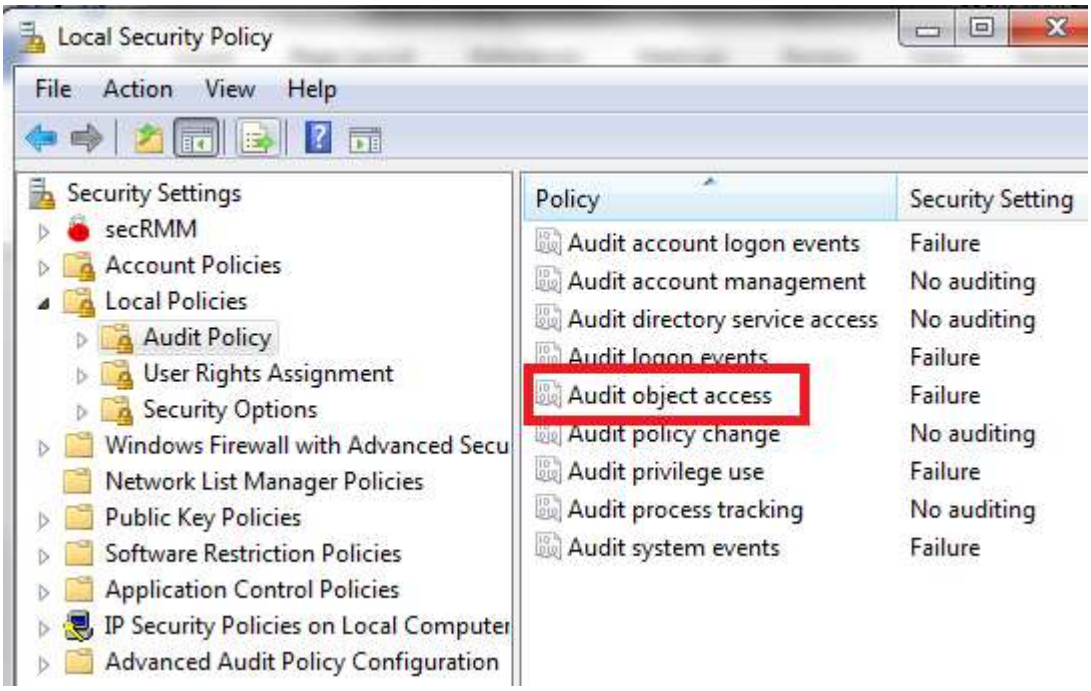


Figure 25 - Invoking "Audit object access"

4. On the "Audit object access Properties" window, check the Success checkbox and then click the OK button at the bottom of the window.

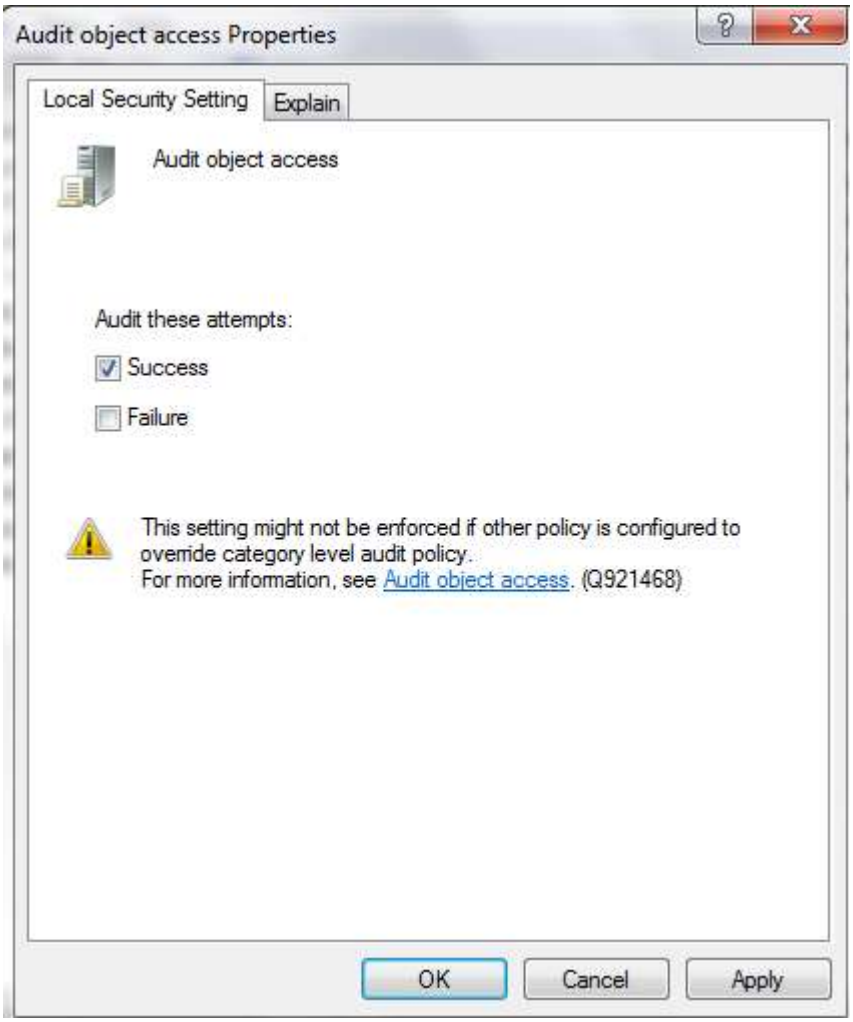


Figure 26 - Audit object access properties dialog

By default, secRMM will write the secRMM events into the Windows security event log as successful events. If you prefer to write the secRMM events into the Windows security event log as failures (instead of successful events), please follow the section below titled "Writing secRMM security events as failures".

Writing secRMM security events as failures

If you would prefer to write the secRMM events into the Windows security event log as failures instead of successes, please:

1. Perform step 4 above again. Click the Failure checkbox instead of the Success checkbox.
2. Follow the section below "Setting the LogSecurityEventsAsFailures property"

Why would you choose to do this step? In a production environment, writing security success events could generate a large amount of events. Therefore, you could choose to only log failures which would minimize the amount of security events generated.

Tools for setting the secRMM properties

secRMM is tightly integrated into the Microsoft technologies that come with the base Operating System and also with the available Microsoft enterprise level tools. This lets you configure secRMM using familiar user interfaces, scripts and tools. The next 4 sub-sections below cover how you can set secRMM properties using the following methods:

1. Microsoft Management Console (MMC Computer Management)
2. Microsoft scripts (Power-shell, VBScript, Jscript, CMD)
3. Active Directory Group Policy Objects (GPO)
4. Microsoft System Center Configuration Manager (SCCM)

MMC SnapIn

The secRMM MMC SnapIn supports the Microsoft MMC version 3.0 console. At a minimum, you will need to have the Microsoft .Net 3.5 framework installed to use the MMC version 3.0 console. The secRMM MMC SnapIn is installed when you install the secRMM product. To access the secRMM MMC SnapIn, go to the Windows "Administrative Tools" menu and select "Computer Management" (see screenshot below).

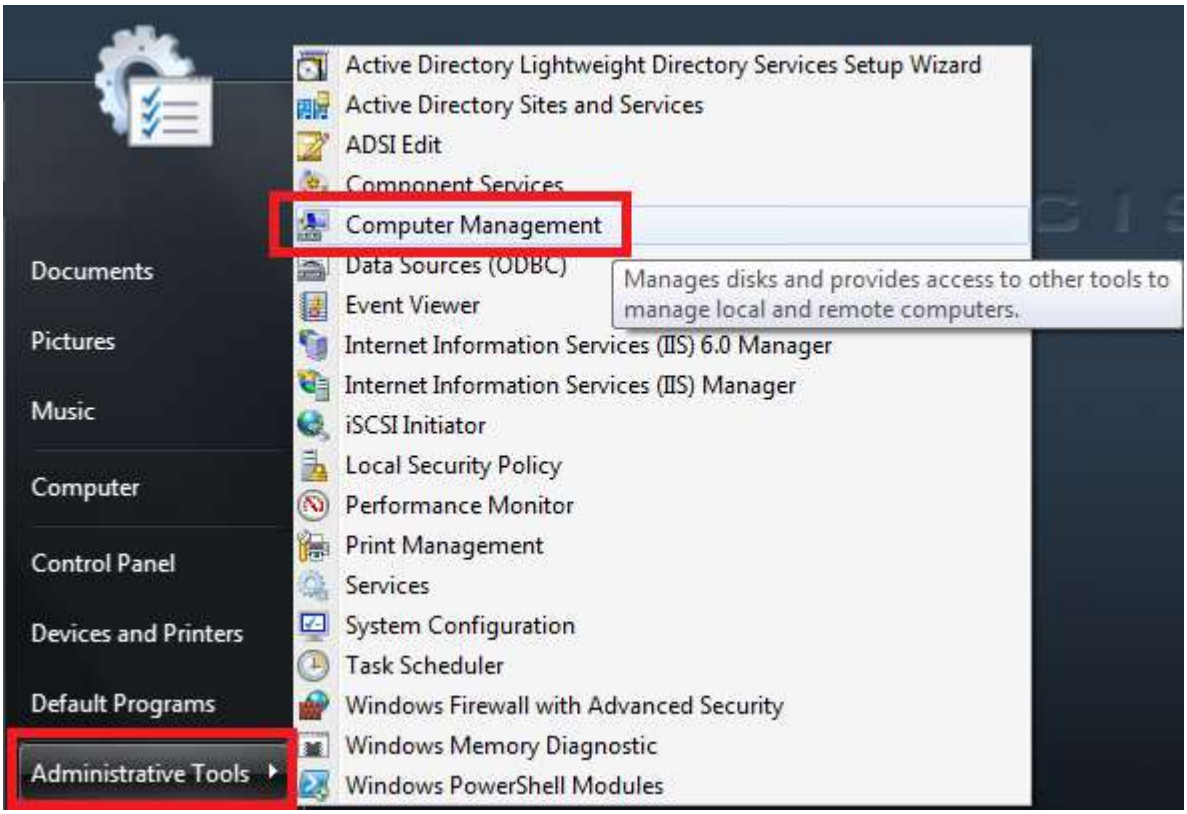


Figure 27 - Invoking the "Computer Management" MMC

The secRMM MMC SnapIn is shown below. To change one of the secRMM properties, simply double click the row. A dialog will open which will allow you to work with the secRMM property. The details of the secRMM properties are in the scripting sections below. To understand a secRMM property, please refer to the appropriate scripting section. The secRMM MMC SnapIn also provides access to the SafeCopy Approver (the two man policy) program, the secRMM Excel 2010 AddIn, information about the secRMM license for

the computer, secRMM Device Tracker and secRMM Configurations. secRMM Configurations let you manage secRMM configurations for the computer configuration and for user configurations.

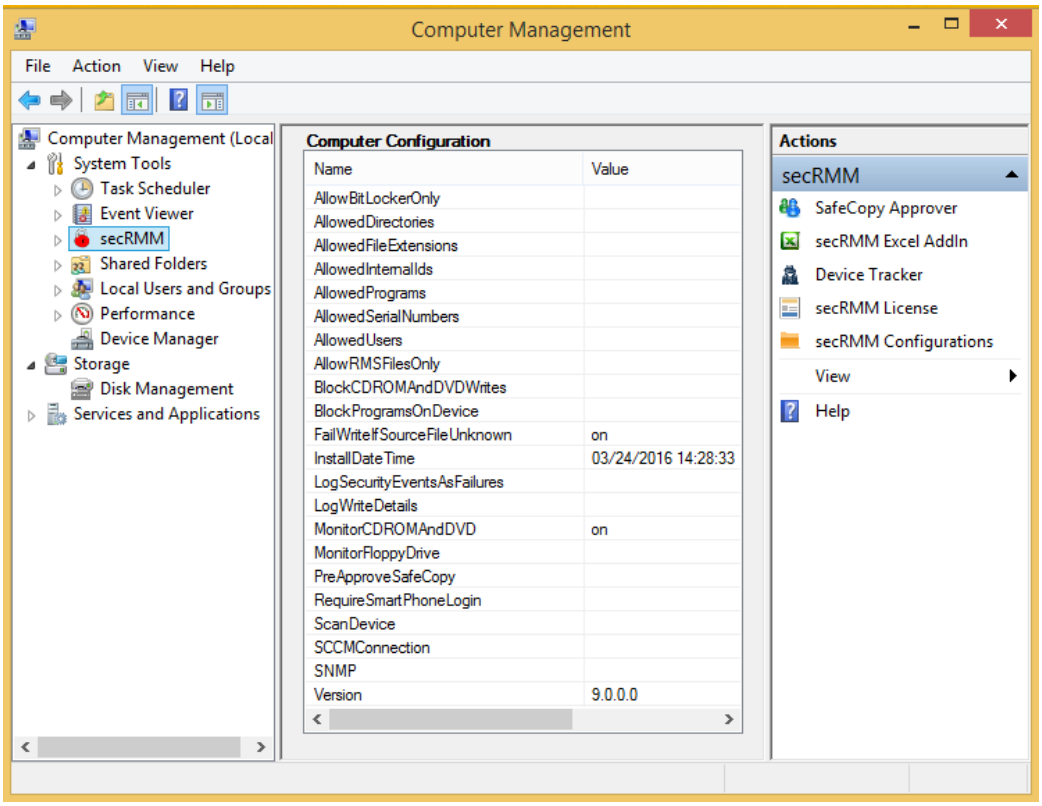


Figure 28 - secRMM MMC SnapIn

secRMM MMC SnapIn Helper Dialogs

The secRMM MMC SnapIn provides helper dialogs for secRMM properties "AllowedDirectories", "AllowedPrograms" and "AllowedUsers". The "AllowedDirectories" helper dialog allows you to select directories using the standard Windows "Browse for Folder" dialog. The "AllowedPrograms" helper dialog allows you to select a program using the standard Windows "File Open" dialog. The "AllowedUsers" helper dialog allows you to select a user from the standard "object picker" dialog (i.e. users list from the local computer and/or Active Directory domain users list).

secRMM Advanced Editor

The secRMM MMC SnapIn provides an "Advanced Editor" for secRMM properties "AllowedDirectories", "AllowedPrograms", "AllowedFileExtensions", "AllowedInternalIds", "AllowedPrograms", "AllowedSerialNumbers" and "AllowedUsers". This editor will take the secRMM semicolon separated property value and list each value on its own row within a single column grid. It lets you add, modify and delete rows. You can also sort the rows in ascending or descending order by single clicking the column header. You can import and export the data as well. Once you hit the OK button in the "Advanced Editor", it will create a single semicolon separated string to go back into the basic secRMM editor.

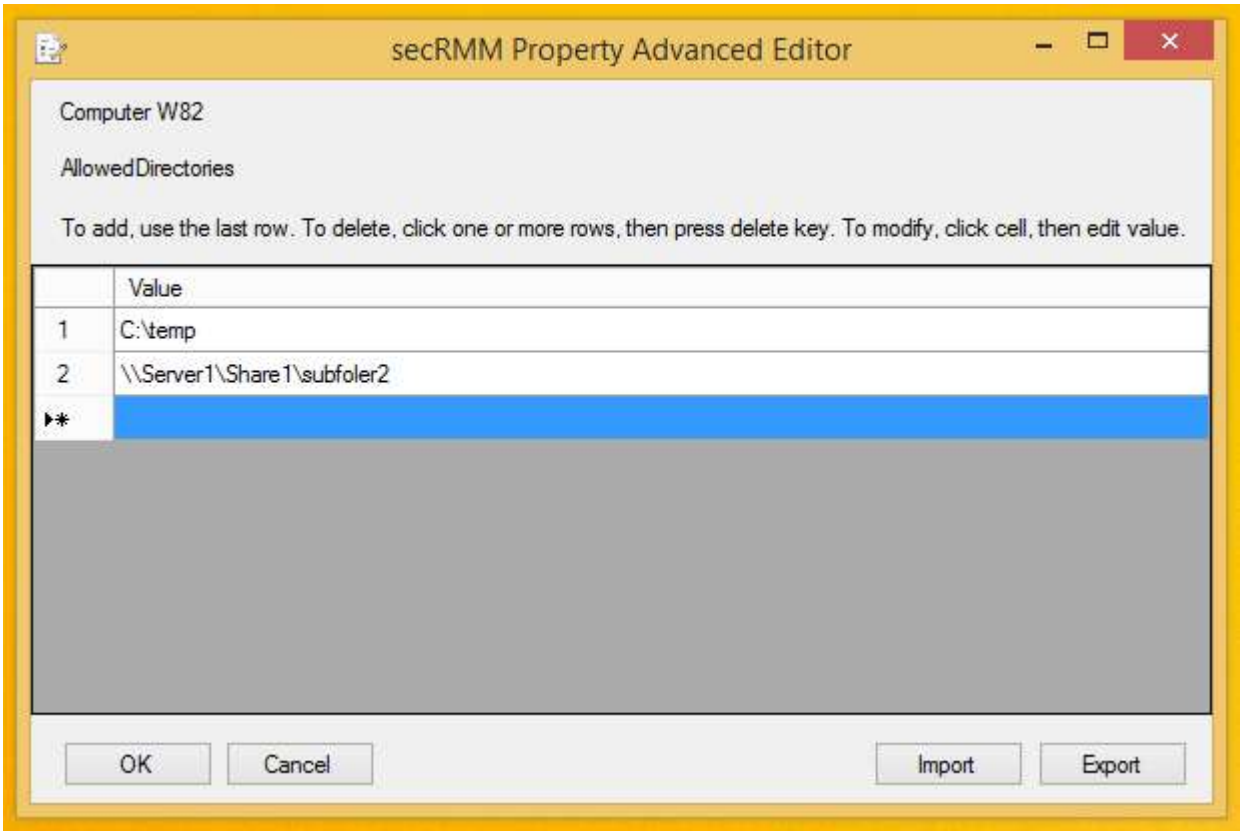


Figure 29 - secRMM Advanced Editor

Connect to another computer

The secRMM MMC SnapIn supports connecting to another computer that has secRMM installed. You do this the same way as the Microsoft MMC SnapIns (such as Event Viewer, Device Manager, etc.) by clicking the root node "Computer Management" and then selecting the action of "Connect to another computer…". Once you are connected to the remote computer, you use the secRMM MMC SnapIn the same way as if you were working locally.

Setting up Connect to another computer

The secRMM MMC SnapIn uses remote WMI to connect to the remote computer. The remote WMI feature depends upon DCOM. Using remote WMI and DCOM may not be configured in your environment. Along with configuring remote WMI and DCOM, you will also likely need to make port exceptions to the firewall. Below are links on the Microsoft site that show you how to configure WMI, DCOM and the firewall. If you need assistance setting this up, please contact Squadra Technologies support or your IT security department.

Connecting to WMI on a Remote Computer

Securing a Remote WMI Connection (DCOM)

Connecting Through Windows Firewall

Below are the commands that will allow you to "Connect to another computer":

```
netsh advfirewall set currentprofile settings remotemanagement enable
netsh advfirewall firewall set rule group="Remote Service Management" new enable=yes
netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes
netsh advfirewall firewall set rule group="Remote Event Log Management" new enable=yes
netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes

REM http://support.microsoft.com/KB/951016
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy
/t REG_DWORD /d 1

REM http://technet.microsoft.com/en-us/library/cc754243.aspx
REM In a WORKGROUP scenario, on the computer where you are doing the "connect to another computer" in
MMC Computer Management:
cmdkey /add:TheNameOfTheComputerYouAreConnectingTo /user:Administrator /pass:??????
```

Active Directory

Group Policy

secRMM properties can be applied using Active Directory Group Policy Objects (AD GPO). secRMM AD GPO supports both Computer and User configurations. If an end-user uses removable media and there is no secRMM User Configuration AD GPO for that user, the secRMM Computer configuration will be applied to that end-user. Using AD GPO to apply secRMM properties is very convenient and useful if you have many users and computers in your environment. You access the secRMM AD GPO using the standard AD GPO Editor as shown in the screenshot below.

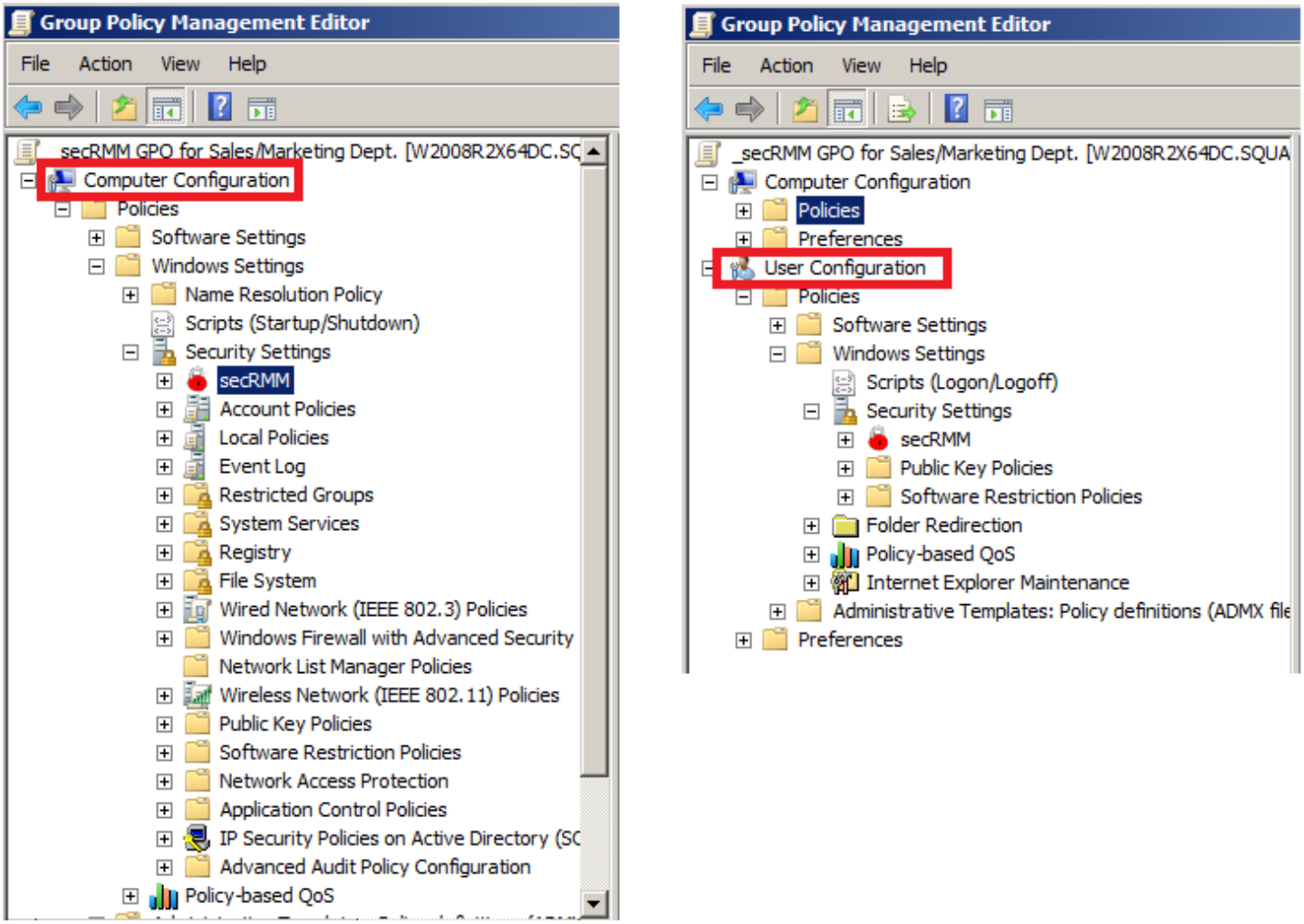


Figure 30 - The AD GPO Editor

secRMM Configurations

When a User Configuration GPO is applied (this happens when a user logs in), secRMM interacts with GPO by creating a specific secRMM User Configuration file for that end-user. If need be, as an Administrator, you can manage the secRMM User Configurations directly from within the secRMM MMC. To do this, you use the MMC action "secRMM Configurations". You can create, delete or modify secRMM User Configurations. While the secRMM AD GPO uses secRMM User Configuration files to implement GPO, you can also create secRMM User Configurations manually by using the secRMM MMC as well. The difference between using secRMM AD GPO vs. manually configuring the secRMM User Configuration file(s) is that GPO will automatically follow the user from machine to machine whereas manually configuring will not. Whether you use GPO or manual configuration will depend on which policy is appropriate for your environment. This same concept is also implemented for System Center Configuration Manager (SCCM).

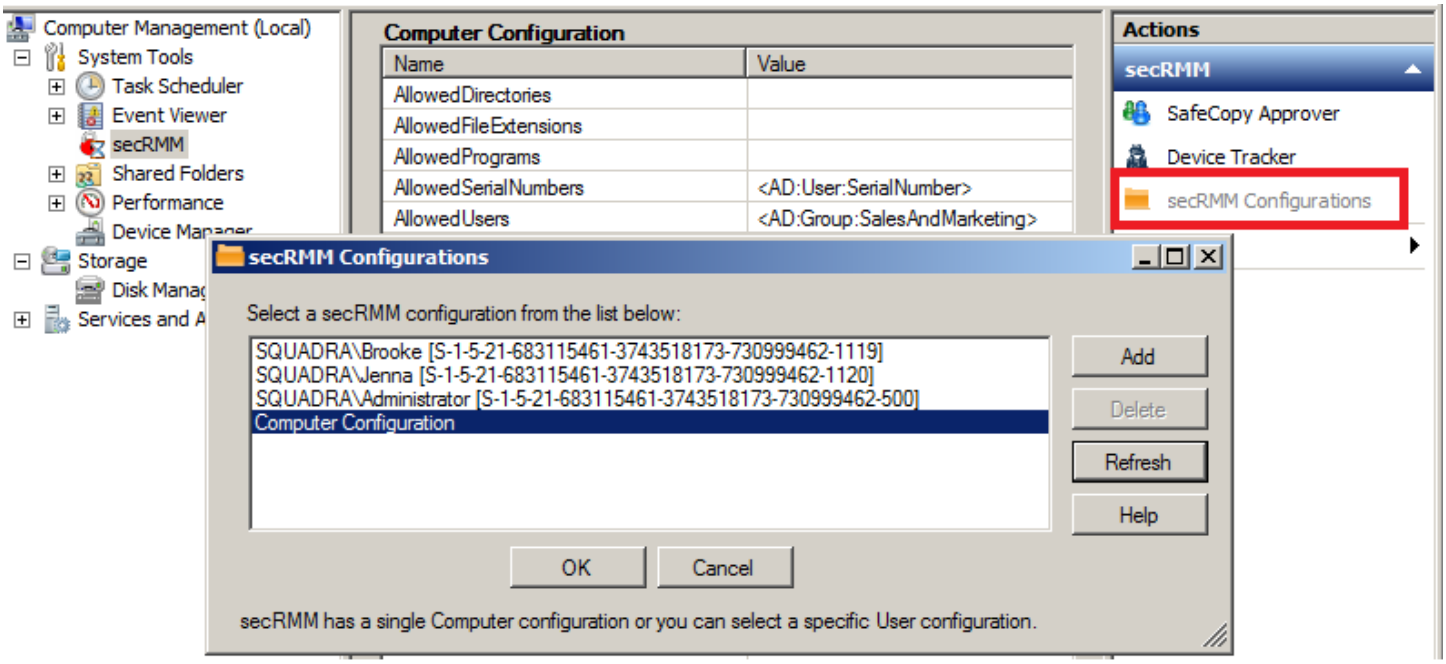


Figure 31 - secRMM Configurations

GPO Security Filtering

When using secRMM via AD GPO, you can filter who (groups of users and/or individual users) the GPO gets applied to by using Security filtering. The most common scenario of when you would use Security filtering is when you define a User Configuration GPO since you have a specific group of users in mind.

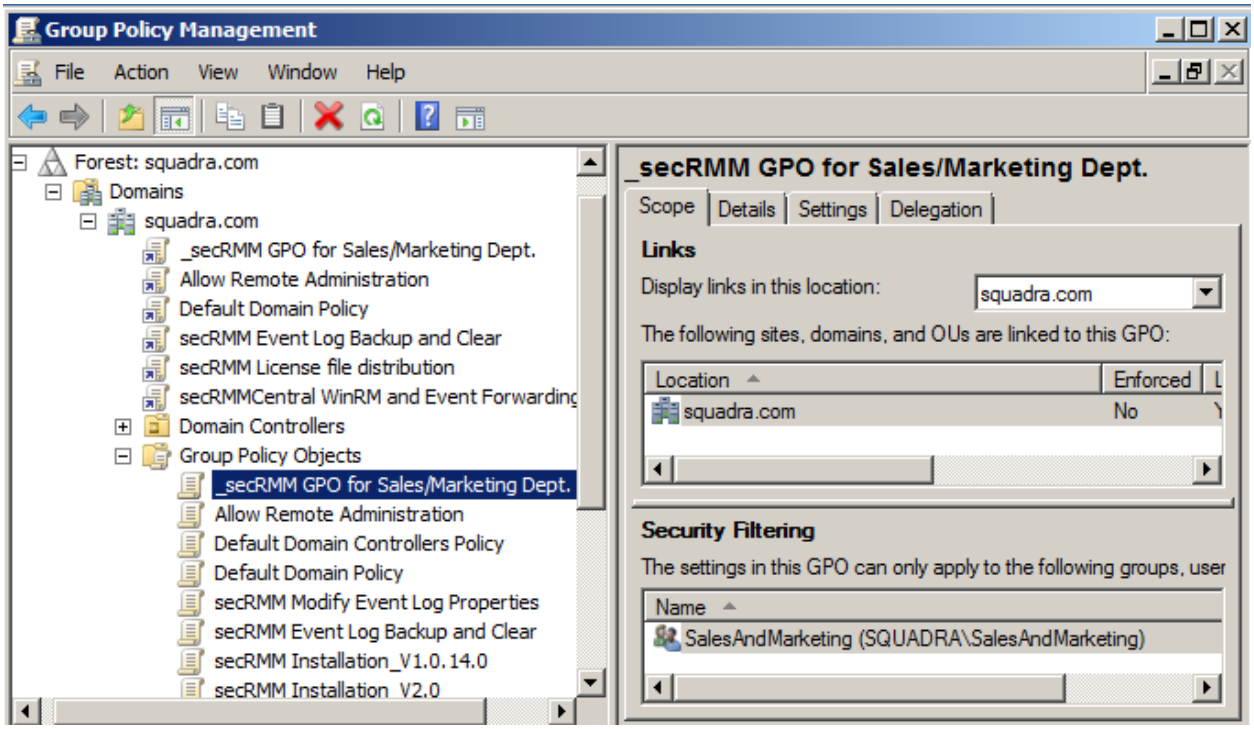


Figure 32 - GPO Security Filtering

GPO WMI Filtering

When using secRMM via AD GPO, you should always apply a WMI filter. The WMI filter for secRMM is shown in the two screenshots below. As you can see, it uses the root\CIMv2 WMI namespace. The WMI Query is SELECT * FROM __NAMESPACE WHERE Name = "secRMM". This WMI filter applies the GPO only to computers that have secRMM installed.

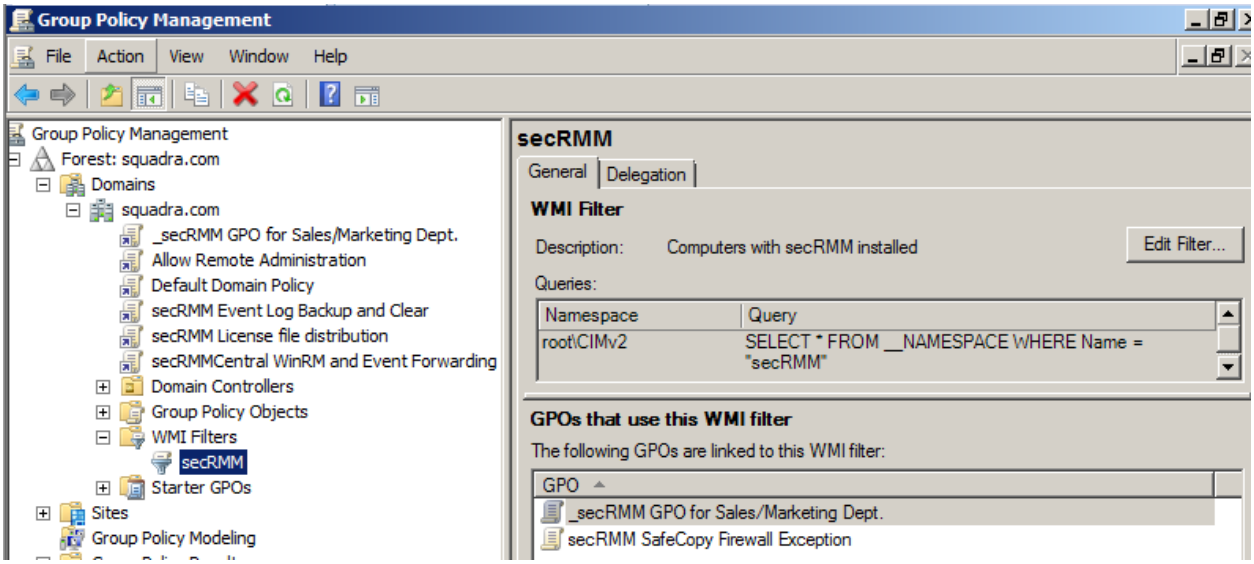


Figure 33 - GPO WMI Filtering

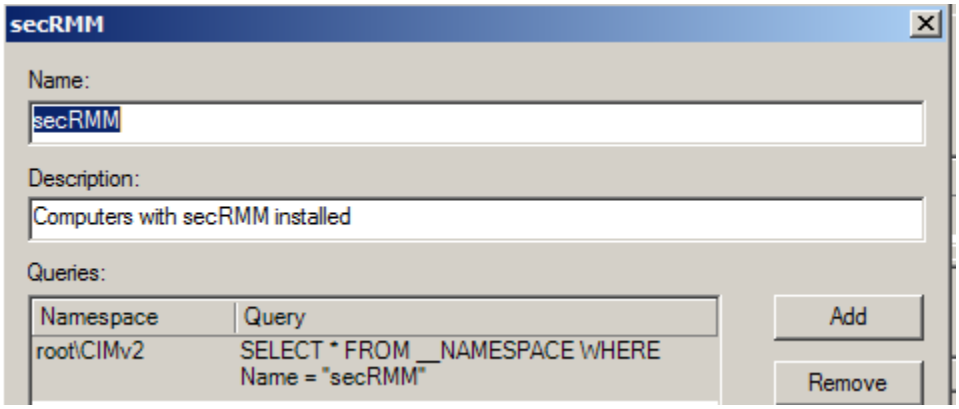


Figure 34 - GPO WMI Query for secRMM

Using AD attributes in secRMM

You can take advantage of using Active Directory (AD) attributes[3]. Integrating AD attributes with secRMM lets you keep your data about your users and computers centralized within the AD database. secRMM can reference any attribute defined on the AD user or AD computer objects. Most all of the attributes can be set to any value you want. To see the complete list of attributes for the user and computer objects, you

[3] When reading documentation on Active Directory, you will also see the documentation use the term properties or variables. So all 3 terms: attributes, properties and variables are all referencing the exact same concept.

use the "Active Directory Users and Computers" MMC as shown in the screenshot below. From within the "Active Directory Users and Computers" MMC, on the main menu bar, select View->Advanced Features.

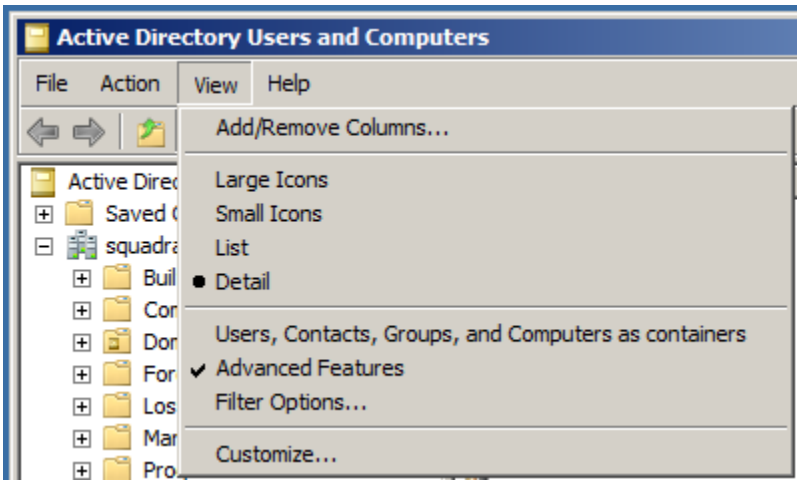


Figure 35 - Enable Advanced Features

Once you have enabled Advanced Features, you can now right mouse click any user (in the Users folder) or computer (in the Computers folder) and select Properties. The Properties dialog is a tabbed dialog. Click the tab named "Attribute Editor". You can set the value of the attribute you wish to use with secRMM. Once you set the Active Directory attribute you want to use, you then specify it in the secRMM property.

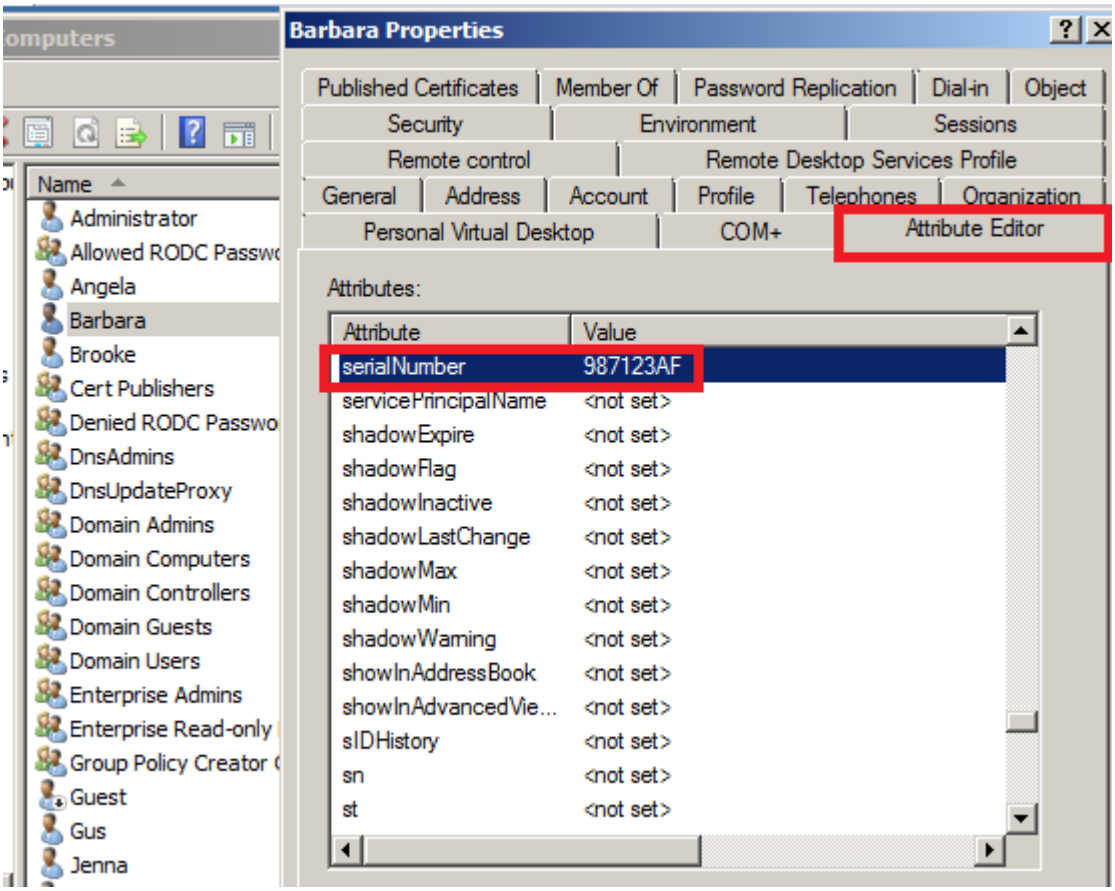
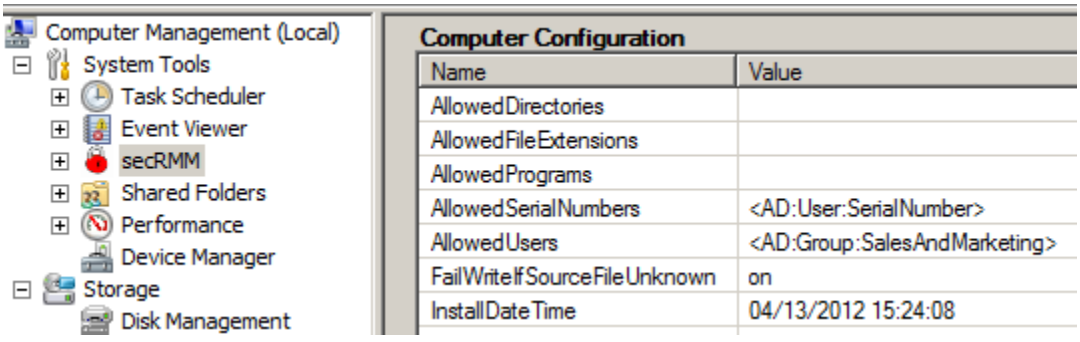


Figure 36 - Active Directory Attribute Editor

As an example, in the screenshot above, we set the serialNumber attribute for user Barbara to the value 987123AF. Now, in the secRMM MMC, we set the secRMM property "AllowedSerialNumber" to be <AD:User:SerialNumber>. At run time then, if Barbara goes to use a removable media device that does not have a serial number of 987123AF, the write operation will fail. For more details on using variables (i.e. AD attributes) in the secRMM properties, please review the section titled "Using variables" above.



System Center Configuration Manager

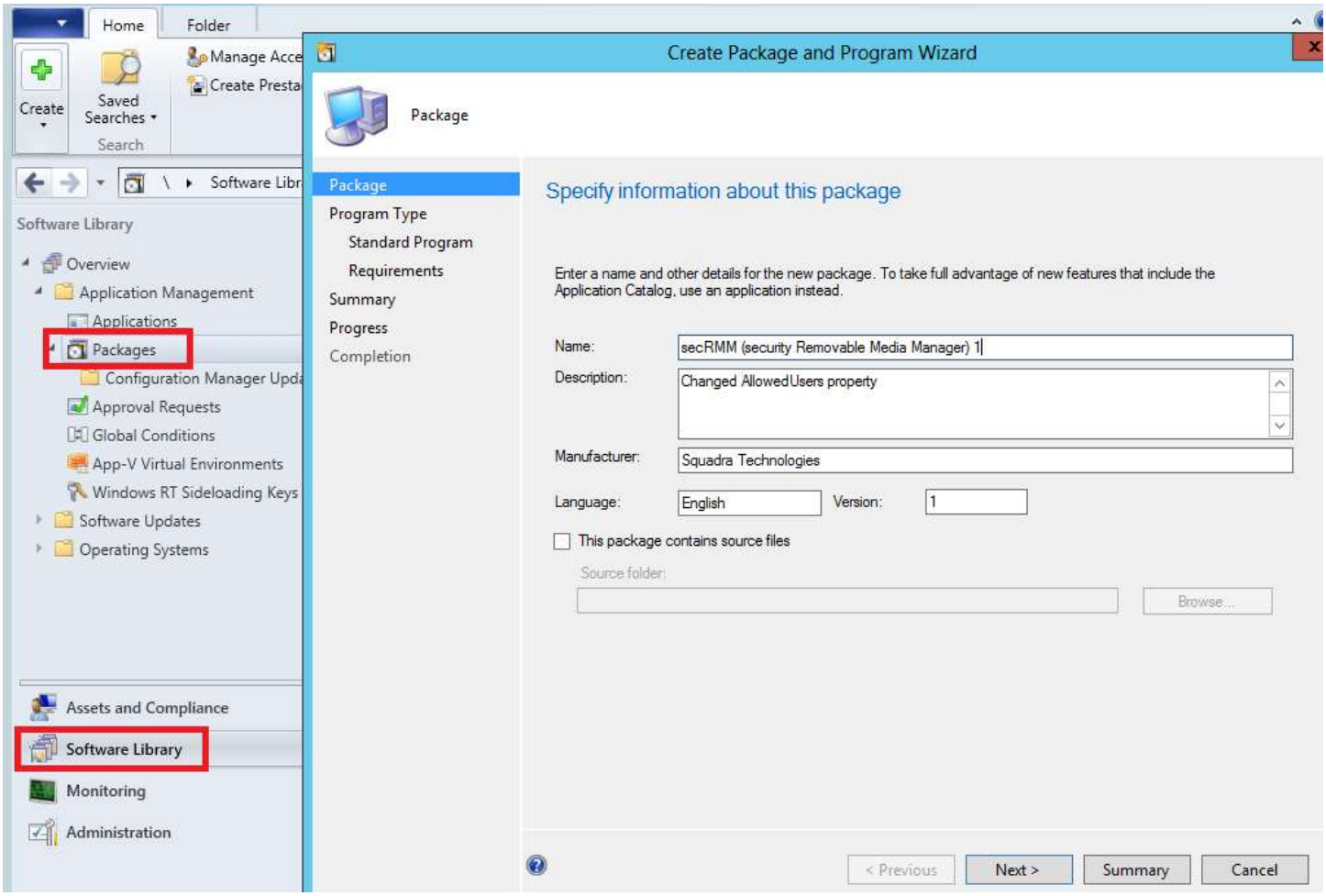
secRMM properties can be applied using System Center Configuration Manager (SCCM). Using SCCM to apply secRMM properties is very convenient and useful if you have many users and computers in your environment.

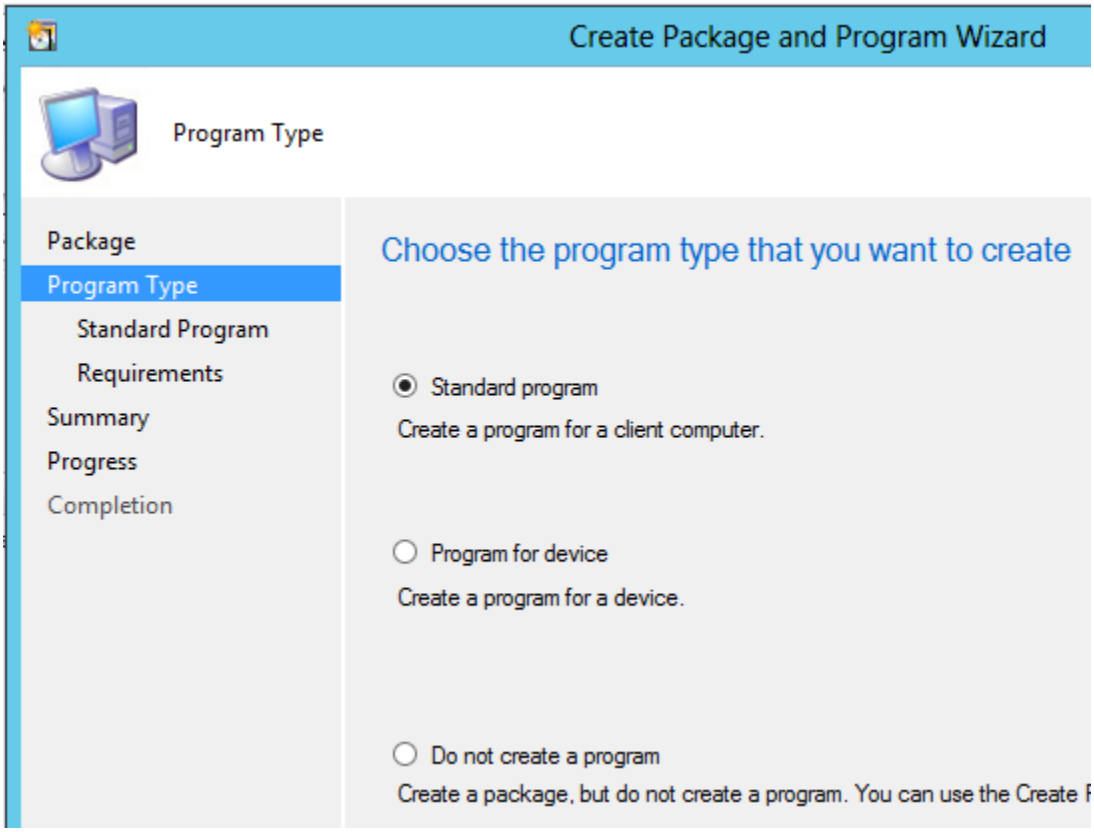
There are 2 options for SCCM:

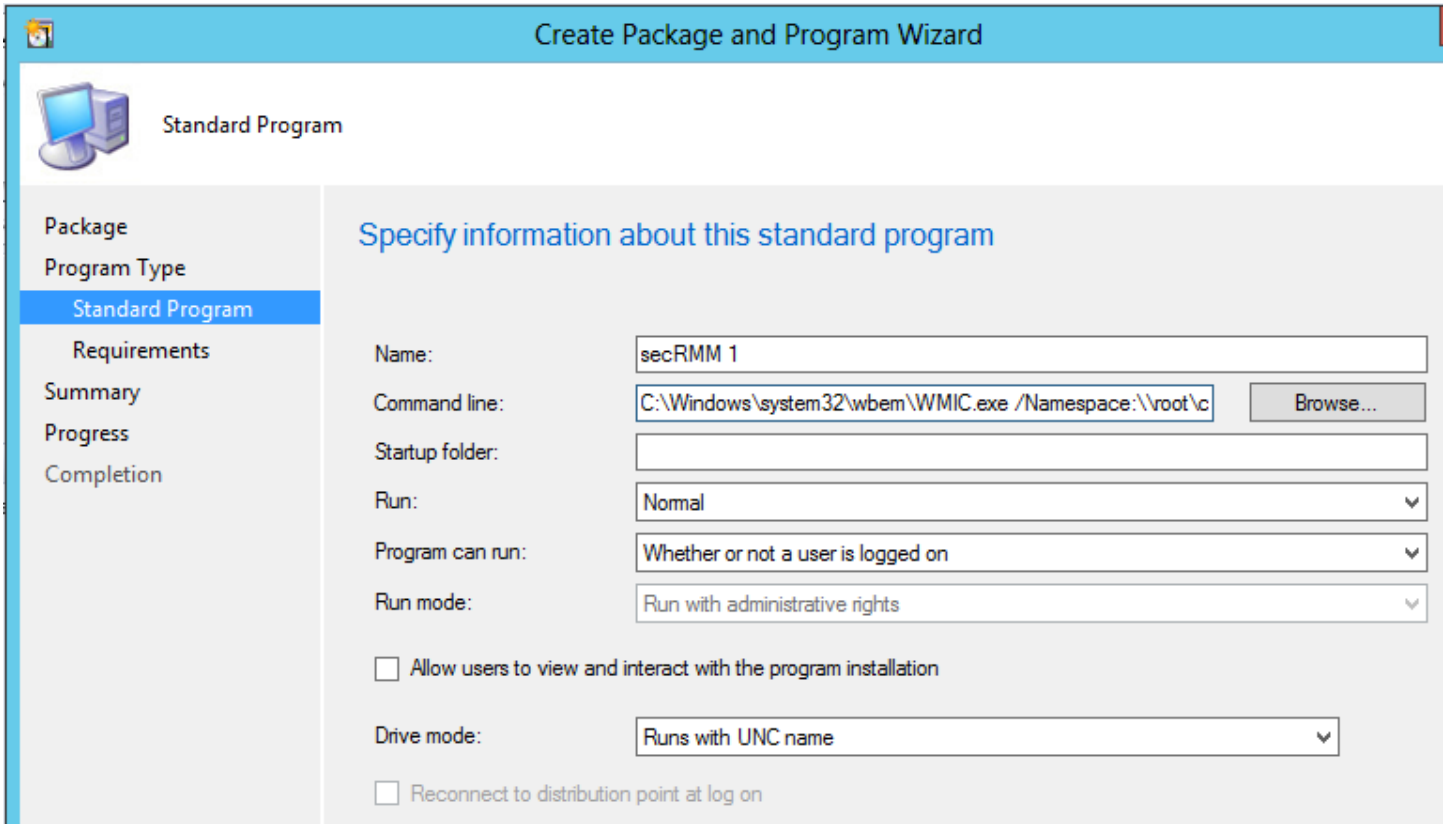
1. Use the secRMM SCCM Console Extension (which uses SCCM Compliance Settings)
   This option requires a separate installation and so is covered in the **SCCM Administrator Guide** which can be downloaded from the Squadra Technologies web site. This is the recommended approach.

2. Use the SCCM Package and Program Wizard. This option is presented below but should only be used if option 1 is not feasible in your environment.

You set the secRMM properties in SCCM using the standard Package/Program wizard as shown in the screenshots below.




Create Package and Program Wizard
Program Type
Package
Program Type
Standard Program
Requirements
Summary
Progress
Completion
Choose the program type that you want to create
Standard program
Create a program for a client computer.
Program for device
Create a program for a device.
Do not create a program
Create a package, but do not create a program. You can use the Create


Create Package and Program Wizard
Standard Program
Package
Program Type
Standard Program
Requirements
Summary
Progress
Completion
Specify information about this standard program
Name:
secRMM 1
Command line:
C:\Windows\system32\wbem\WMIC.exe /Namespace:\\root\c
Browse...
Startup folder:
Run:
Normal
Program can run:
Whether or not a user is logged on
Run mode:
Run with administrative rights
Allow users to view and interact with the program installation
Drive mode:
Runs with UNC name
Reconnect to distribution point at log on

The key item is the "Command line". You will use the following syntax:

C:\Windows\system32\wbem\WMIC.exe /Namespace:\\root\cimv2\secRMM path secRMMWMIProvider call SetProperty "ConfigMgr", "Property Name", "Property Value", ""

Where "Property Name" is one of the secRMM properties that show up in the Computer Management MMC. "Property Value" is the value you want to set for the "Property Name".

Scripts

For scripting, you can choose to use any COM supported Windows scripting language (VBscript, Jscript, Powershell, or third party developed scripts such as ActiveState Perl). secRMM intentionally supports scripting for any automation scenarios you might need. You may also use Windows batch script (CMD files).

Under the secRMM product directory (by default, this will be \Program Files\secRMM), there is a subfolder named AdminUtils. This subfolder holds various scripts which help in configuring the secRMM product. The scripts in this subfolder are pointed out in the "secRMM properties" section and subsections below.

secRMM properties

This section and its subsections provide the details of each secRMM property. The secRMM properties control how secRMM operates.

Overview

The following table lists the name of each secRMM property and gives a brief description of the purpose of the property.

Name	Description
Allow BitLocker Only	This property is either on or off. When on, secRMM will block file copies to any removable media device that does not have Microsoft BitLocker technology enabled. If a user attempts to copy a file to a device that does not have BitLocker enabled, secRMM will block the file copy and create a "failed write attempt" event log record with an event id of 513 (ALLOW BITLOCKER ONLY ACTIVE).
Allowed Directories	This property is a semicolon separated list of directories. These are the only directories that secRMM will allow file copies from. Therefore, if a user attempts to copy a file from a directory that is not in this list, secRMM will block the file copy and create a "failed write attempt" event log record with an event id of 504 (SOURCE DIRECTORY AUTHORIZATION).
Allowed File Extensions	This property is a semicolon separated list of file extensions (note, you do not need to include the period). These are the only file extensions that secRMM will allow file copies from. Therefore, if a user attempts to copy a file whose file extension is not in this list, secRMM will block the file copy and create a "failed write attempt" event log record with an

	event id of 504 (SOURCE FILE EXTENSION AUTHORIZATION).
Allowed Internal Ids	This property is a semicolon separated list of internal ids. Internal ids are unique strings that describe the vendor of the device and the product name of the device. The industry refers to these 2 items as VIDs and PIDs. VIDs is short for vendor id. PIDs is short for product id. Therefore, if you want to only allow devices from a particular vendor, you would specify the unique VID. If you wanted to only allow particular devices types (i.e. specific model from the vendor) from a particular vendor, you would specify the VID and PID. These are the only devices that secRMM will allow file copies to. Therefore, if a user attempts to copy a file to a device that is not in this list, secRMM will block the file copy and create a "failed write attempt" event log record with an event id of 506 (INTERNAL ID AUTHORIZATION).
Allowed Programs	This property is a semicolon separated list of programs (note, you should specify the complete path of the program, not just the file name). These are the only programs that secRMM will allow to copy files to removable media. Therefore, if a user attempts to copy a file using a program that is not in this list, secRMM will block the file copy and create a "failed write attempt" event log record with an event id of 501 (PROGRAM AUTHORIZATION).
Allowed Serial Numbers	This property is a semicolon separated list of device serial numbers. These are the only devices that secRMM will allow file copies to. Therefore, if a user attempts to copy a file whose serial number is not in this list, secRMM will block the file copy and create a "failed write attempt" event log record with an event id of 502 (SERIAL # AUTHORIZATION).
Allowed Users	This property is a semicolon separated list of Windows user ids. These are the users that secRMM will allow to copy files to removable media. Therefore, if a user attempts to copy a file who is not in this list, secRMM will block the file copy and create a "failed write attempt" event log record with an event id of 500 (USER AUTHORIZATION).
AllowRMSFilesOnly	This property is either on or off. When on, secRMM will block file copies to any removable media device when the file being copies is not protected by the Microsoft RMS technology. If a user attempts to copy a file to a device that is not RMS protected, secRMM will block the file copy and create a "failed write attempt" event log record with an event id of 514 (ALLOW RMS FILES ONLY ACTIVE).
Block CDROM and DVD Writes	This property will block file copies (from Windows explorer) to CDs and DVDs. The user is still able to read from the device. Therefore, if a user attempts to copy a file to the CD/DVD, secRMM will block the file copy and create a "failed write attempt" event log record with an event id of

	511 (BLOCK CD/DVD ACTIVE).
Block Programs On Device	This property will block programs that reside on the removable storage device from executing. The user is still able to read and copy files from the device. If there is an attempt to execute a program that resides on the device, secRMM will block the execution of the program and create a "failed program execution attempt" event log record with an event id of 514 (BLOCK PROGRAM EXECUTION ACTIVE).
FailWriteIfSourceFileUnknown	This property will block file copies when secRMM cannot determine the complete file path of the file the user is trying to copy to the removable media device. If this condition occurs, secRMM will block the file copy and create a "failed write attempt" event log record with an event id of 503 (UNKNOWN SOURCE). This property is the only secRMM property that comes enabled at installation time.
Install Date/Time	This property is the date and time when secRMM was installed onto the computer. It is a display only property and cannot be modified.
Log Security Events As Failures	This property is either on or off. When on, secRMM will log the secRMM events into the Windows security event log in addition to the secRMM event log.
Log Write Details	This property is either on or off. When on, secRMM will log the file copy START TIME. secRMM always logs the file copy END TIME. Turning this property on is not recommended in production environments.
Monitor CDROM and DVD	This property is either on or off. When on, secRMM will log the file copy events for CD/DVD devices.
Monitor Floppy Drive	This property is either on or off. When on, secRMM will log the file copy events for floppy drives.
PreApproveSafeCopy	This property is either on or off. When on, secRMM will block the start of SafeCopy until an "approver" allows the user to use SafeCopy.
RequireSmartPhoneLogin	This property is either on or off. When on, secRMM will not mount the mobile device to the computer unless the user has provided the proper credentials. The user provides the proper credentials by specifying his userid and password on the mobile device via the secRMM mobile app. This is an optional security feature.
ScanDevice	This property is either on or off. When on, secRMM will start a malware scan of the device when it is connected to the Windows computer. This feature uses Microsoft Defender (previously named Endpoint Protection) to perform the scan.

SCCMConnection	This property provides the credentials required for secRMM to forward its event data into Microsoft System Center Configuration Manager (SCCM).
SNMP	This property tells secRMM where to send SNMP traps. The SNMP traps contain the same data as the secRMM event records that go into the Windows secRMM event log.
Version	This property is the secRMM version that is installed on the computer. It is a display only property and cannot be modified.

Using variables

This section describes the power of using variables within specific secRMM properties. Variables are a powerful way to narrow down the use of removable media by specifying the "from where", "to what" and "by whom" conditions in a very simple manner. Specifically, the 3 secRMM properties that allow variables are:

1. AllowedDirectories (specifies where files can be copied from on the local or network drives)
2. AllowedSerialNumbers (which removable media devices are allowed to be used)
3. AllowedUsers (which users are allowed to write to removable media devices)

A variable within the secRMM property starts with a < character and ends with a > character. The secRMM MMC has a helper dropdown listbox that provides a convenient way to insert variables into the secRMM properties. You can use the following variables:

1. UserId
2. Domain
3. Computer
4. Any Active Directory (AD) user attribute
5. Any Active Directory (AD) computer attribute
6. Local User Group
7. Active Directory User Group

You can arrange the variables in any way that matches your environment.

The table below shows which variable (the rows) is appropriate for which secRMM property (the columns):

	AllowedDirectories	AllowedSerialNumbers	AllowedUsers
UserId	X		X
Domain	X		X
Computer	X		
AD user property	X	X	
AD computer property	X	X	
Local User Group			X
AD User Group			X

Here are some examples of using variables within the secRMM properties:

1. AllowedDirectories is set to C:\Users\<UserId>;\\Server1\Share1\<AD:User:Department>
2. AllowedSerialNumbers is set to <AD:User:SerialNumber>
3. AllowedUsers is set to <AD:Group:SalesAndMarketing>

For more details on using AD attributes, please review the section titled " Using AD attributes in secRMM" above.

The AllowedUsers AD:Group variable can be overridden so that you can insert the complete LDAP query rather than use just a simple Group name that is defined directly under the users container. This lets you have subcontainers within the LDAP query, for example:

<AD:Group:CN=USB_Users,OU=Special Groups,OU=ABC Groups,DC=ABC,DC=COM>

Setting the FailWriteIfSourceFileUnknown property

To enable the FailWriteIfSourceFileUnknown feature, you can run the VBScript in the AdminUtils subfolder that is named SetFailWriteIfSourceFileUnknown.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "FailWriteIfSourceFileUnknown", True
```

The secRMM property FailWriteIfSourceFileUnknown is the only secRMM property that comes enabled at installation time.

Setting the LogSecurityEventsAsFailures property

To enable the LogSecurityEventsAsFailures feature, you can run the VBScript in the AdminUtils subfolder that is named SetLogSecurityEventsAsFailures.vbs. If you open this VBScript in your favorite editor (or

notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "LogSecurityEventsAsFailures", True
```

NOTE: If you do enable this property, be sure you follow the section above titled "Writing secRMM security events as failures".

Setting the LogWriteDetails property

By default, secRMM only writes the "write completed" event for each file. This is done to minimize the amount of events. However, you may be interested in seeing when the write starts. If you would like to capture the "write start" events as well as the "write completed" events, you need to enable the LogWriteDetails secRMM property.

To enable the LogWriteDetails property, you can run the VBScript in the AdminUtils subfolder that is named SetLogWriteDetails.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "LogWriteDetails", True
```

Enabling Authorization

There are eight secRMM properties which control authorization. Authorization uses userids, programs, serial numbers, internal Ids (VIDs and PIDS), directories and file extensions to control writing to removable media devices.

Authorizing Users

To enable the AllowedUsers property, you can run the VBScript in the AdminUtils subfolder that is named SetAllowedUsers.vbs. Before you run the VBScript, you must edit the script and change the value of the property to accommodate your environment. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to the list of users you want to give authorization to. Remember here, that this list of users will be the only users allowed to write to any removable media device for this particular computer. Any other user will be denied. For all denied users, secRMM will generate an event 500. If you need multiple users, separate them with a semicolon. To turn this property off, you would change the list of users to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "AllowedUsers", "Squadra\Barbara"

Example of specifying multiple users:
objSecRMM.SetProperty "AllowedUsers", _
"Squadra\Barbara;Squadra\Angela;Squadra\Brooke;Squadra\Jenna"
```

```
Notice the underscore (_) on the first line of the "specifying multiple users" example.  In VBScript,
an underscore is a line continuation.
```

The AllowedUsers property supports using "local group" and "Active Directory group" attributes. Please review the section titled "Using AD attributes in secRMM" above.

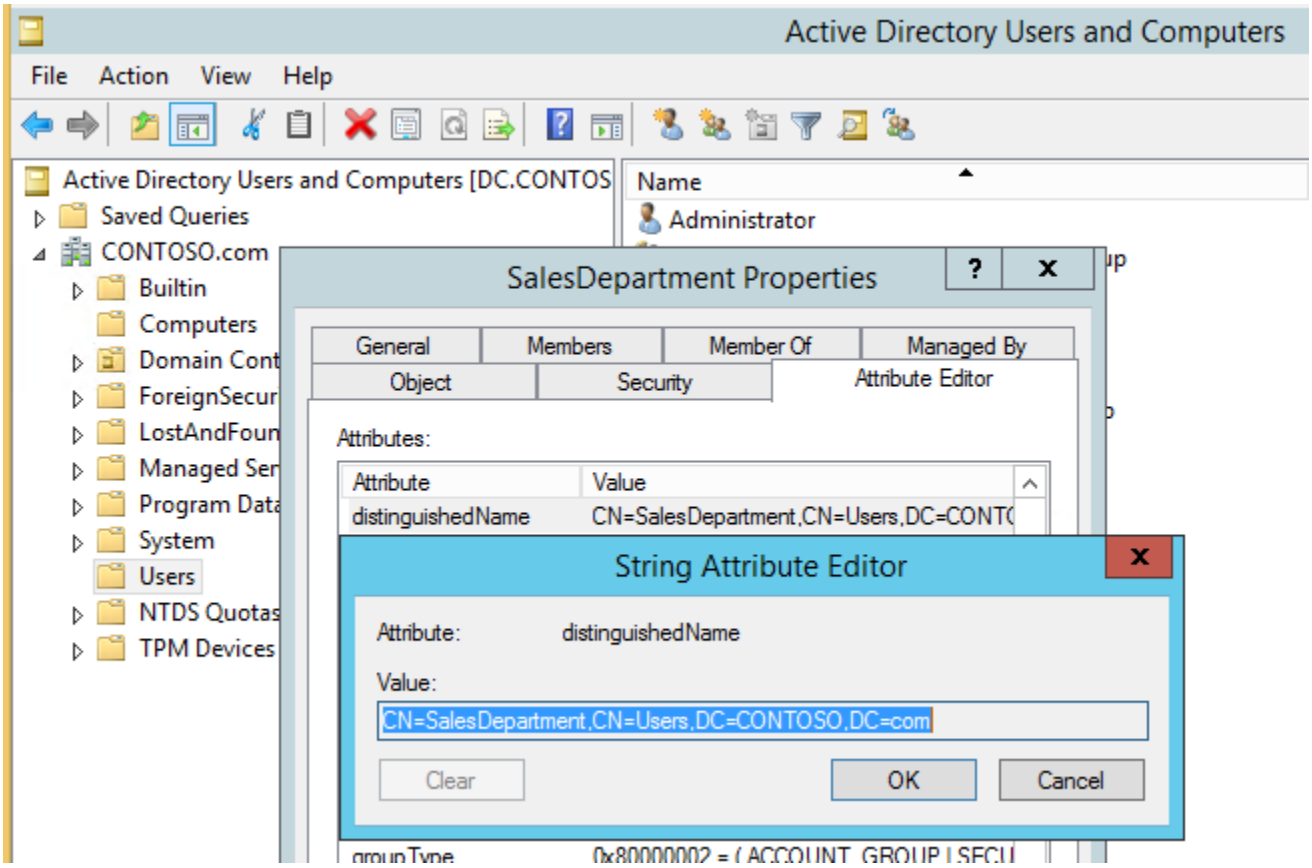
The AllowedUsers property is one of four secRMM properties (AllowBitLockerOnly, AllowedSerialNumbers, AllowedInternalIds, AllowedUserIds) that can have secRMM perform an authorization check when the Removable Media device is plugged into the computer (i.e. a secRMM ONLINE event). To do this from within a script, place the text **[EnforceWhenPluggedIn]** at the front of the "AllowedUsers" property value:

```
objSecRMM.SetProperty "AllowedUsers", "[EnforceWhenPluggedIn]Squadra\Barbara"
```

The AllowedUsers AD:Group variable can be overridden so that you are allowed to insert the complete LDAP query rather than use just a simple Group name that is defined directly under the users container. This lets you have subcontainers within the LDAP query, for example:

<AD:Group:CN=USB_Users,OU=Special Groups,OU=ABC Groups,DC=ABC,DC=COM>

To get this value, you can use the Active Directory "Attribute Editor" on the "user group". The attribute to use is the "distinguishedName" as shown in the screen shot below.



Authorizing Programs

To enable the AllowedPrograms property, you can run the VBScript in the AdminUtils subfolder that is named SetAllowedPrograms.vbs. Before you run the VBScript, you must edit the script and change the value of the property to accommodate your environment. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to the list of programs you want to give authorization to. Remember here, that this list of programs will be the only programs allowed to write to any removable media device for this particular computer. Any other program will be denied. For all denied programs, secRMM will generate an event 501. If you need multiple programs, separate them with a semicolon. To turn this property off, you would change the list of programs to Null and then run the VBScript again.

Notice that to prevent program spoofing, you need to specify the complete path to the program.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "AllowedPrograms", "c:\windows\explorer.exe"

Example of specifying multiple programs:
objSecRMM.SetProperty "AllowedPrograms", _
"C:\Windows\system32\cmd.exe;c:\windows\explorer.exe;C:\Program Files\Microsoft
Office\Office14\excel.exe"
```

Notice the underscore (_) on the first line of the "specifying multiple programs" example. In VBScript, an underscore is a line continuation.

Note that this script allows you to pass in the program name from the command line as well. This script is defined this way so the secRMM installation can set SafeCopy as the allowed program.

Authorizing Serial Numbers

To enable the AllowedSerialNumbers property, you can run the VBScript in the AdminUtils subfolder that is named SetAllowedSerialNumbers.vbs. Before you run the VBScript, you must edit the script and change the value of the property to accommodate your environment. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to the list of serial numbers you want to give authorization to (i.e. to be allowed to write to these removable media devices). Remember here, that this list of serial numbers will be the only removable media devices allowed to be written to for this particular computer (or user). Any other removable media devices will be denied. For all denied serial numbers, secRMM will generate an event 502. If you need multiple serial numbers, separate them with a semicolon. To turn this property off, you would change the list of serial numbers to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "AllowedSerialNumbers", "12345678"

Example of specifying multiple serial numbers:
objSecRMM.SetProperty "AllowedSerialNumbers", _
"12345678;1234567A;1234567B"

Notice the underscore (_) on the first line of the "specifying multiple serial numbers" example.  In
VBScript, an underscore is a line continuation.
```

The AllowedSerialNumbers property supports using attributes from Active Directory. A common use is to map a specific removable media device to a specific user. This works well in environments where the user is assigned a removable media device for use but the device is not to be used by any other user (i.e. a 1-to-1 mapping of user to device). Please review the section titled "Using AD attributes in secRMM" above.

The AllowedSerialNumbers property is one of four secRMM properties (AllowBitLockerOnly, AllowedSerialNumbers, AllowedInternalIds, AllowedUserIds) that can have secRMM perform an authorization check when the Removable Media device is plugged into the computer (i.e. a secRMM ONLINE event). To do this from within a script, place the text **[EnforceWhenPluggedIn]** at the front of the "AllowedSerialNumbers" property value:

```
objSecRMM.SetProperty "AllowedSerialNumbers","[EnforceWhenPluggedIn]72BC27;1234567A;1234567B"
```

CD/DVD devices do not have true serial numbers. If you want to include the CD/DVD device, you can specify "**CD_DVD**".

Authorizing Internal Ids

To enable the AllowedInternalIds property, you can run the VBScript in the AdminUtils subfolder that is named SetAllowedInternalIds.vbs. Before you run the VBScript, you must edit the script and change the value of the property to accommodate your environment. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to the list of internal Ids you want to give authorization to (i.e. to be allowed to write to these removable media devices). Remember here, that this list of internal Ids will be the only removable media devices allowed to be written to for this particular computer. Any other removable media devices will be denied. For all denied internal Ids, secRMM will generate an event 506. If you need multiple interal Ids, separate them with a semicolon. To turn this property off, you would change the list of internal Ids to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "AllowedInternalIds", "VID_04e8&PID_6860"

Example of specifying multiple internal Ids:
objSecRMM.SetProperty "AllowedInternalIds", _
"VID_04e8&PID_6860;VID_04e8&PID_6875;&VEN_CBM&PROD_USB_2.0_FLASH"
```

The AllowedInternalIds property is one of four secRMM properties (AllowBitLockerOnly, AllowedSerialNumbers, AllowedInternalIds, AllowedUserIds) that can have secRMM perform an authorization check when the Removable Media device is plugged into the computer (i.e. a secRMM ONLINE event). To do this from within a script, place the text **[EnforceWhenPluggedIn]** at the front of the "AllowedInternalIds" property value:

```
objSecRMM.SetProperty " AllowedInternalIds ","[EnforceWhenPluggedIn]&VEN_CBM&PROD_USB_2.0_FLASH"
```

The primary purpose of the AllowedInternalIds property is to limit removable media use to a particular USB manufacturer and/or to specific models/product lines of usb drives. Every USB device is assigned a Vendor ID (VID) and Product ID (PID). The VID and PID are contained within the secRMM Internal ID along with other relevant data about the device. You can think of USB VIDs and PIDs equivalent to the various car companies and the different car models each of them manufacture.

For an un-official list of USB VIDs and PIDs, please see http://www.linux-usb.org/usb.ids. If you do not see the USB manufacturer on this list, you will need to contact the manufacturer of your device. Alternatively, you can generate a secRMM ONLINE event and look at the Internal Id that gets generated.

Authorizing Directories

To enable the AllowedDirectories property, you can run the VBScript in the AdminUtils subfolder that is named SetAllowedDirectories.vbs. Before you run the VBScript, you must edit the script and change the value of the property to accommodate your environment. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to the list of directories you want to give authorization to (i.e. to be allowed to copy files from these directories). Any other directories will be denied. For any denied directories, secRMM will generate an event 504. If you need multiple directories, separate them with a semicolon. To turn this property off, you would change the list of directories to Null and then run the VBScript again.

For the AllowedDirectories property, you can use predefined variables (<UserId>, <Domain> and <Computer> as well as attributes from Active Directory) when specifying a directory. These variables will be replaced during the secRMM authorization phase. For example, if you specify a directory C:\Users\<UserId> then if a user named John tries to copy a file to a removable media device, he can only copy files from the directory C:\Users\John. The <Domain> variable is the Netbios (short name) of the domain. The <Computer> variable is the Netbios (short name) of the local computer. To use attributes from Active Directory, please review the section titled "Using AD attributes in secRMM" above.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "AllowedDirectories", "C:\temp"

Example of specifying multiple directories:
objSecRMM.SetProperty " AllowedDirectories", _
"C:\temp;D:\"
```

Authorizing File Extensions

To enable the AllowedFileExtensions property, you can run the VBScript in the AdminUtils subfolder that is named SetAllowedFileExtensions.vbs. Before you run the VBScript, you must edit the script and change the value of the property to accommodate your environment. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to the list of file extensions you want to give authorization to (i.e. to be allowed to copy files with the extension you specify). Any other file extensions will be denied. For any denied file extensions, secRMM will generate an event 505. If you need multiple file extensions, separate them with a semicolon. To turn this property off, you would change the list of file extensions to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "AllowedFileExtensions", "doc"

Example of specifying multiple file extensions:
objSecRMM.SetProperty " AllowedFileExtensions", _
"doc;xls"
```

Authorizing only BitLocker devices

Using Microsoft BitLocker to encrypt and password protect removable media is a very common scenario. secRMM can be made to only allow BitLocker enabled devices to be written to. The secRMM property that enables this is called AllowBitLockerOnly.

To enable or disable the AllowBitLockerOnly property, you can run the VBScript in the AdminUtils subfolder that is named SetAllowBitLockerOnly.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "AllowBitLockerOnly", True
```

For any device that is not BitLocker protected and has a write attempt, secRMM will generate an event 513.

The AllowBitLockerOnly property is one of four secRMM properties (AllowBitLockerOnly, AllowedSerialNumbers, AllowedInternalIds, AllowedUserIds) that can have secRMM perform an authorization check when the Removable Media device is plugged into the computer (i.e. a secRMM ONLINE event). To do this from within a script, place the text **[EnforceWhenPluggedIn]** at the front of the "AllowBitLockerOnly" property value (notice the word "on" after):

```
objSecRMM.SetProperty "AllowBitLockerOnly ","[EnforceWhenPluggedIn]on"
```

If the [EnforceWhenPluggedIn] is enabled, secRMM will generate an event 512 when a nonBitLocker device is mounted. The device will also be ejected so that the Windows Operating System cannot see it.

Authorizing only RMS protected files

Using Microsoft Rights Management Services (RMS) is a very powerful DLP solution since the security protection is embedded directly within the file containing the data you wish to protect. secRMM can be made to only allow RMS protected files to be written to removable storage devices. The secRMM property that enables this is called AllowRMSFilesOnly.

Microsoft RMS must be setup in your domain, it is not available by default. For Microsoft documentation on RMS, please see https://technet.microsoft.com/en-us/library/cc771234(v=ws.10).aspx.

To enable or disable the AllowRMSFilesOnly property, you can run the VBScript in the AdminUtils subfolder that is named SetRMSFilesOnly.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "AllowRMSFilesOnly", True
```

For any file that is not RMS protected and has a write attempt, secRMM will generate an event 515.

Preventing programs from executing on devices

By default, secRMM allows users to execute programs that reside on the removable storage device. The BlockProgramsOnDevice property can prevent them from doing this.

To enable or disable the BlockProgramsOnDevice property, you can run the VBScript in the AdminUtils subfolder that is named SetBlockProgramsOnDevice.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "BlockProgramsOnDevice", True
```

For any program on the device that attempts to execute, secRMM will generate an event 514.

Scanning devices for malware

The ScanDevice property will start a malware scan of the device when it is connected to the Windows computer. The feature uses the Microsoft Defender program to perform the scan.

To enable or disable the ScanDevice property, you can run the VBScript in the AdminUtils subfolder that is named SetScanDevice.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "ScanDevice", True
```

secRMM will generate an event 300 indicating the result of the scan.

Monitoring CDROM/DVD and/or Floppy drives

By default, secRMM does monitor writing to the CD/DVD device when using Windows Explorer (see the Windows Explorer screen shots below). Windows allows using a CD/DVD either like a "USB flash drive" or "With a CD/DVD player". Microsoft documentation refers to these format options as "Live File System" and "Mastered" respectively. secRMM monitors the CD/DVD device for both of these format options.

secRMM does not (by default) monitor Floppy drives. You can enable having secRMM monitor or not monitor these devices by specifying the "MonitorCDROMAndDVD" and/or "MonitorFloppyDrive" properties.

To enable or disable the MonitorCDROMAndDVD property, you can run the VBScript in the AdminUtils subfolder that is named SetMonitorCDROMAndDVD.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "MonitorCDROMAndDVD", True
```

To enable the MonitorFloppyDrive property, you can run the VBScript in the AdminUtils subfolder that is named SetMonitorFloppyDrive.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "MonitorFloppyDrive", True
```

Block writing to CDROM/DVD

You can also prevent file writes to CDROM and DVDs.

To prevent file writes to CDROM and DVDs, you can run the VBScript in the AdminUtils subfolder that is named SetBlockCDROMAndDVDWrites.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
```

```
objSecRMM.SetProperty "BlockCDROMAndDVDWrites", True
```

The BlockCDROMAndDVDWrites property can also be set to have secRMM enforce the rule when the CD/DVD is inserted into the Windows computer (called "Eject Mode"). To set secRMM Eject Mode for CD/DVDs, you would change the 3rd line to:

```
objSecRMM.SetProperty "BlockCDROMAndDVDWrites", "[EnforceWhenPluggedIn]on"
```

Finalizing a CDROM/DVD

When you use Windows Explorer to copy files to a CD/DVD disc, the disc remains writeable. If you need to prevent the disc from being written to again, you can run the secRMM FinalizeDisc program. The FinalizeDisc program is located in the UserUtils subdirectory (by default, this is C:\Program Files\secRMM\UserUtils). To run FinalizeDisc, open a cmd window and type:
"C:\Program Files\UserUtils\FinalizeDisc" E:
where E: is the drive letter of your CD/DVD.

Setting the SCCMConnection property

The SCCMConnection property provides the System Center Configuration Manager (SCCM) credentials (i.e. server/userid/password) so that secRMM can communicate with SCCM. When this property is set, secRMM will forward the secRMM event data to SCCM. SCCM will store the secRMM event data as SCCM "status messages". For security purposes, there is no secRMM script to set this property. Please use the *secRMM SCCM 2012 Administrator Guide* which can be downloaded from the Squadra Technologies web site for instructions on how to set the SCCMConnection property.

Setting the SNMP property

To enable the SNMP feature, you can run the VBScript in the AdminUtils subfolder that is named SetSNMP.vbs. If you open this VBScript in your favorite editor (or notepad), you will see the SNMP properties that you need to set. Unlike the other secRMM scripts, this script is a bit longer since configuring SNMP requires several SNMP properties to be set instead of just one. The last VBScript line sets the property to SNMP enabled. To turn secRMM SNMP off, you would change the word strSecRMMSNMP to Null and then run the VBScript again.

Specific SNMP details are discussed in the SNMP subsection under the section titled "Integrating secRMM data into your environment".

Setting the PreApproveSafeCopy property

To enable the PreApproveSafeCopy feature, you can run the VBScript in the AdminUtils subfolder that is named SetPreApproveSafeCopy.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "PreApproveSafeCopy", True
```

When the PreApproveSafeCopy property is set to true, the secRMM SafeCopy end-user GUI application will force the end-user to get "pre-approval" before the program can be used by the end-user (i.e. a two man policy). Please see the section below titled SafeCopy for further details.

Setting the RequireSmartPhoneLogin property

To enable the RequireSmartPhoneLogin feature, you can run the VBScript in the AdminUtils subfolder that is named RequireSmartPhoneLogin.vbs. If you open this VBScript in your favorite editor (or notepad), you will see it is 3 lines of VBScript code (see below). The last VBScript line sets the property to true (or on). To turn this property off, you would change the word True to Null and then run the VBScript again.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "RequireSmartPhoneLogin", True
```

When the RequireSmartPhoneLogin property is set to true, secRMM will force the end-user to first login to Active Directory (or the local Windows computer in non-Active Directory environments) from the smartphone they want to use as removable media storage. This requires that the end-user have the secRMM smartphone app installed on their smartphone. The secRMM smartphone app is currently available on Android, Apple and BlackBerry.

Preventing write activity to Removable Media – Lockdown mode

While Microsoft provides the ability to prevent end-users from using Removable Media devices (for instructions on Microsoft's approach, please review KB article 823732 on the Microsoft MSDN web site), you can use secRMM to prevent end-users from writing to Removable Media devices. To use secRMM to prevent end-users from writing to Removable Media devices, simply provide an invalid value for any one of the secRMM authorization properties. The trick is to provide a value that will never match (i.e. authorize). A simple value to use is the word "invalid" (so that you remember that you are providing an invalid value). Below is the script showing an example of this by using the "AllowedSerialNumbers" secRMM property. Since it is not realistic for a removable media device to have a serial number that is the word invalid, secRMM will prevent any write activity to the removable media devices.

```
Dim objSecRMM
Set objSecRMM = CreateObject("secRMMInterface")
objSecRMM.SetProperty "AllowedSerialNumbers", "invalid"
```

This method of preventing write activity to Removable Media devices is called secRMM Lockdown mode. SecRMM Lockdown mode can be set at secRMM installation and you can enable it and disable it at any time after installation. As a convenience, there is a script provided in the AdminUtils subfolder called SetLockdownMode.vbs. You can use this at any time to put secRMM into Lockdown mode. Note that the script SetLockdownMode.vbs sets the secRMM "AllowedSerialNumbers" property to "secRMM_is_locked_down". The secRMM MMC GUI also puts the value of "secRMM_is_locked_down" into the AllowedSerialNumbers property. Using secRMM Lockdown mode is especially useful when you configure secRMM to use the secRMM SafeCopy end-user GUI application. secRMM SafeCopy is discussed in the next section.

SafeCopy

Introduction

SafeCopy works in conjunction with secRMM to provide a higher level of security and monitoring of removable media write activity. The SafeCopy user interface mimics the standard Windows explorer program but only allows writing to removable media[4] and adjusts what it displays to the end-user based on secRMM properties. Administrators can enable secRMM/SafeCopy to enforce a two man policy. A two man policy means at least 2 people must be involved for the removable media write operation to occur. The two man policy is a common operating procedure in many critical military situations.

SafeCopy sends the actions that the end-user is performing within SafeCopy to secRMM. secRMM then logs this data into the Security and secRMM event logs (SNMP traps are also generated if secRMM SNMP is configured).

The subsections below describe how to set secRMM properties that effect the operation of SafeCopy.

Apple mobile device copying files to and from Windows

The SafeCopy program exposes the complete file system of an apple mobile device (in addition to the other non-apple mobile devices and the standard USB devices) without having to use iTunes. This makes the apple mobile device file system available to enterprise users who need to copy files to and from the apple mobile device and Windows.

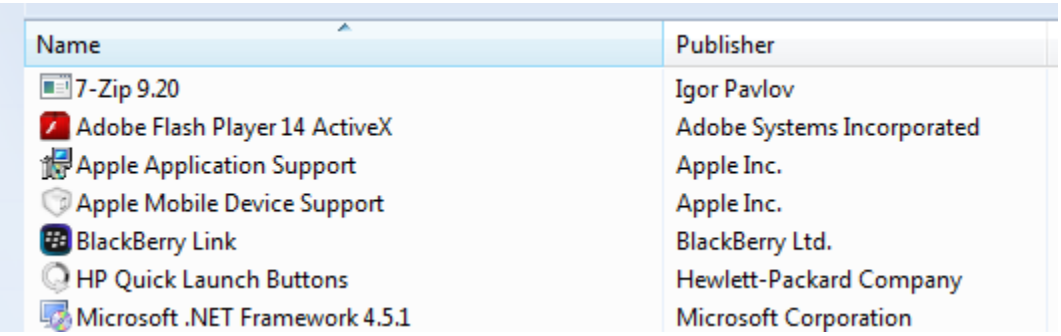
In addition to the apple functionality provided with secRMM SafeCopy, secRMM also ships with a collection of apple utilities developed by the libimobiledevice Unix community. These apple utilities are under the secRMM installation folder at AdminUtils\AppleUtils. The libimobiledevice utilities are very useful when using apple mobile devices within an enterprise environment.

Note, that starting with IOS 8.3, Apple has unfortunately locked down the App data directories unless the App was built with the UIFileSharingEnabled flag set.

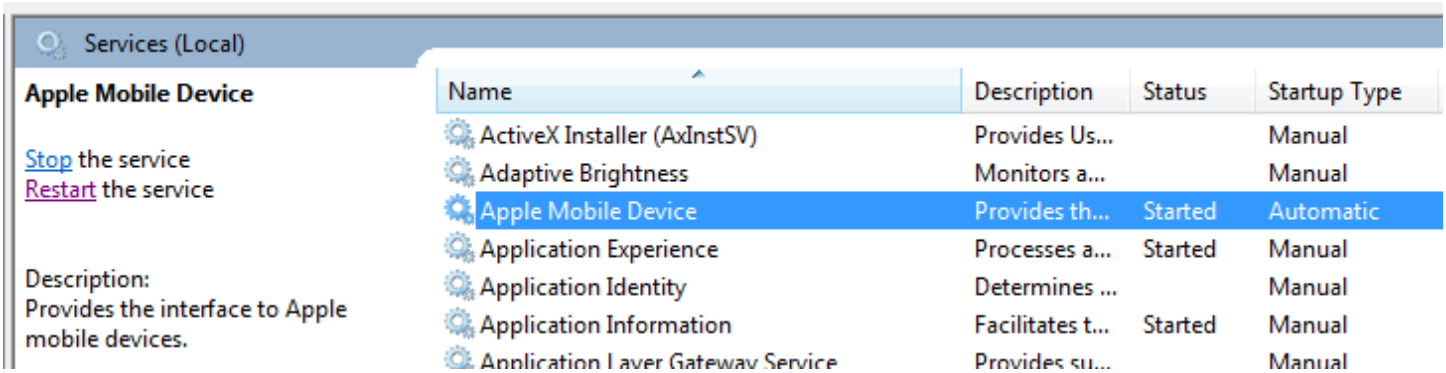
Installing the apple device drivers onto Windows without installing iTunes

If you need this type of apple functionality in your environment, you will first need to install the apple device drivers on the Windows computer running secRMM SafeCopy. The apple device driver installation is contained within two Windows installer files (i.e. files with an msi extension) that are provided by the iTunesSetup[64].exe file which is downloaded from the apple iTunes web site. The iTunesSetup[64].exe file is actually a zip file so you can open it with a zip program such as 7-Zip. Extract the msi files: AppleApplicationSupport.msi and AppleMobileDeviceSupport[64].msi. Install the AppleApplicationSupport.msi and then the AppleMobileDeviceSupport[64].msi. After you install the msi files, you can use SafeCopy with your apple mobile devices. If you look in your Windows Add/Remove Programs, it should have the two apple installations as shown in the screenshot below.

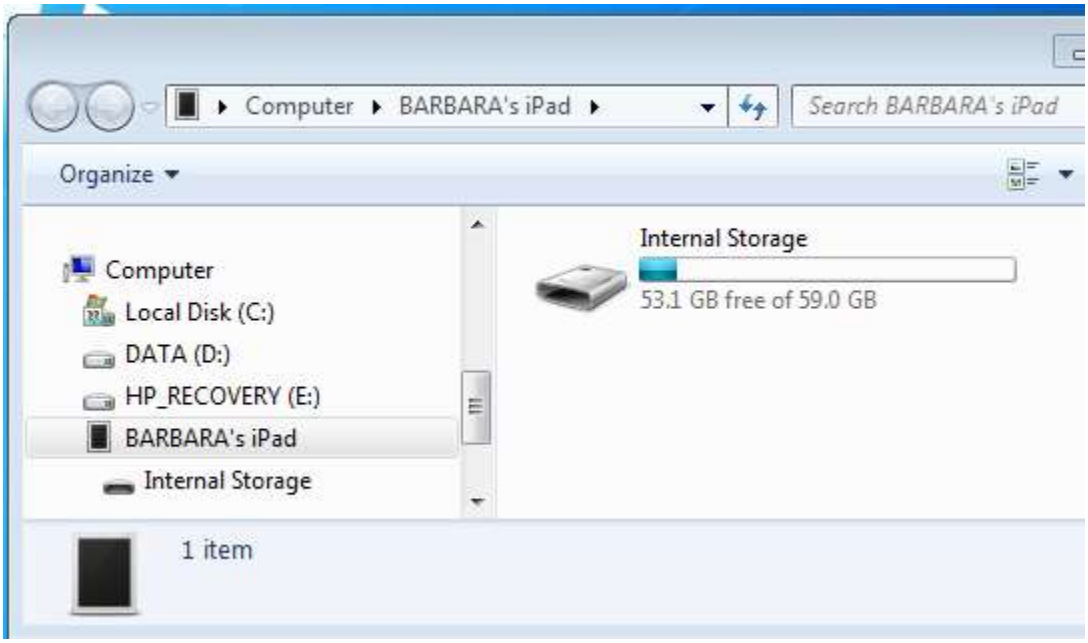
[4] You can also copy from the removable media using "Drag-and-Drop" only.



Additionally, in the list of Windows services, you will see one apple service named "Apple Mobile Device".



For secRMM SafeCopy to be able to see the apple mobile device attached via the USB cable, the Windows operating system must be able to see it first. You will know that the Windows operating system is recognizing the apple mobile device because Windows Explorer will show you the device as shown in the screen shot below.



Preapproval (two man policy)

Configuration

To enforce a two man policy, you set the secRMM property "PreApproveSafeCopy" to true. You should also set the secRMM property "AllowedPrograms" to only be the SafeCopy program (if you installed secRMM to the default installation directory, it will be the value C:\Program Files\secRMM\UserUtils\secRMMSafeCopy.exe). Within the secRMM MMC, there is a helper button for SafeCopy on the AllowedPrograms dialog (as shown in the screenshot below). Clicking the SafeCopy helper button will insert the full path and name of SafeCopy into the AllowedPrograms secRMM property.

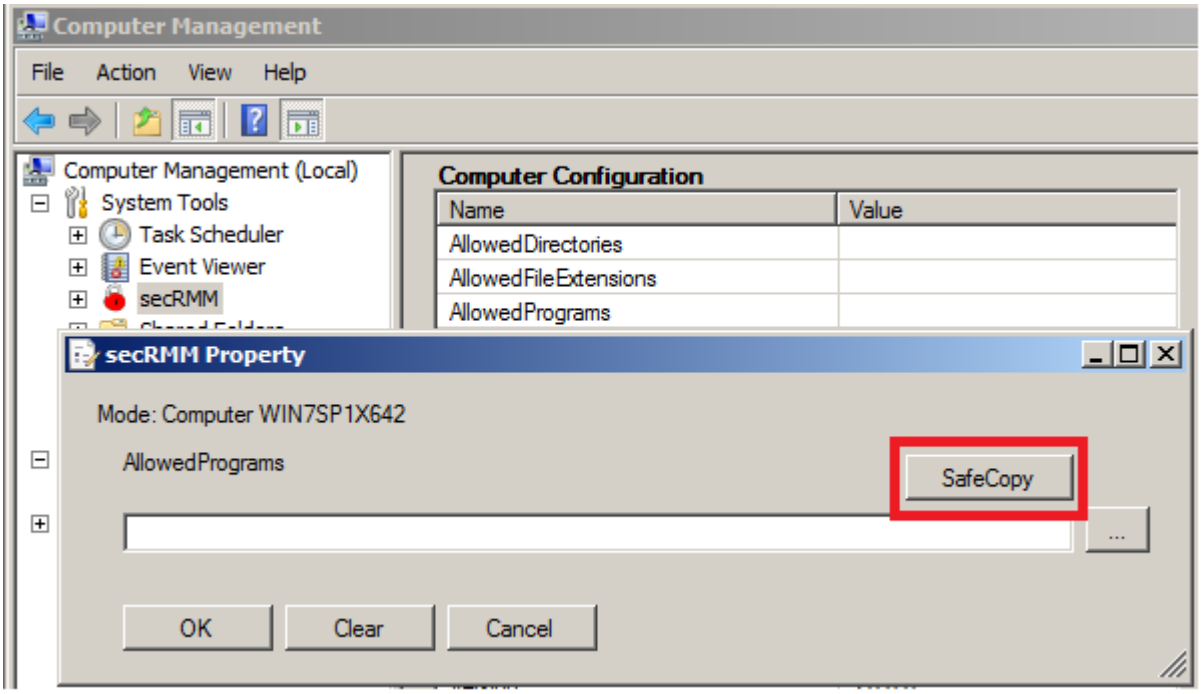


Figure 37 - SafeCopy AllowedPrograms helper button

End-User Experience

When the end-user starts SafeCopy under the two man policy, the following dialog will display:

Figure 38 - end-user experience when PreapproveSafeCopy is set on

Modifying the message to the end-user

The message that is displayed to your end-users should reflect the instructions required for your environment. The message is in html format and is in the file named secRMMSafeCopyContactInfo.html in the secRMM subfolder named UserUtils (if you installed secRMM to the default installation directory, it will be the value C:\Program Files\secRMM\UserUtils\secRMMSafeCopyContactInfo.html).

Performing the approval

By default, an Administrator of the computer where SafeCopy is running must approve the use of SafeCopy. To perform the approval, run the program named secRMMSafeCopyApprover.exe which is located in the secRMM subfolder named AdminUtils (if you installed secRMM to the default installation directory, it will be the value C:\Program Files\secRMM\ AdminUtils\secRMMSafeCopyApprover.exe). You can also call secRMMSafeCopyApprover.exe from the secRMM MMC SnapIn Actions list or from the secRMM Excel AddIn.

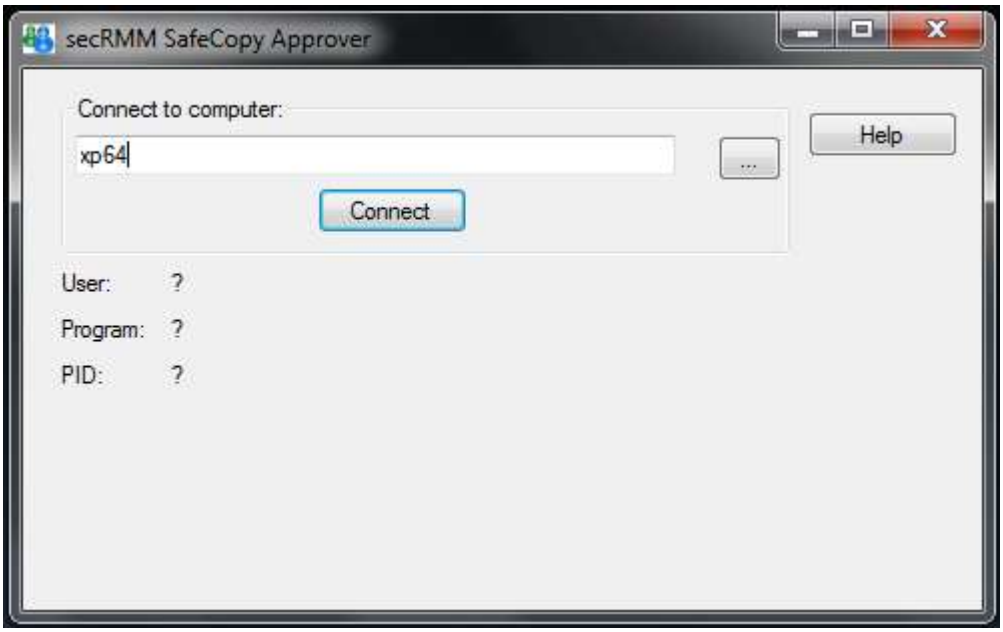


Figure 39 - Dialog to perform the approval, before connecting

Connect to the computer where SafeCopy is running by specifying the computer name and then clicking the connect button.

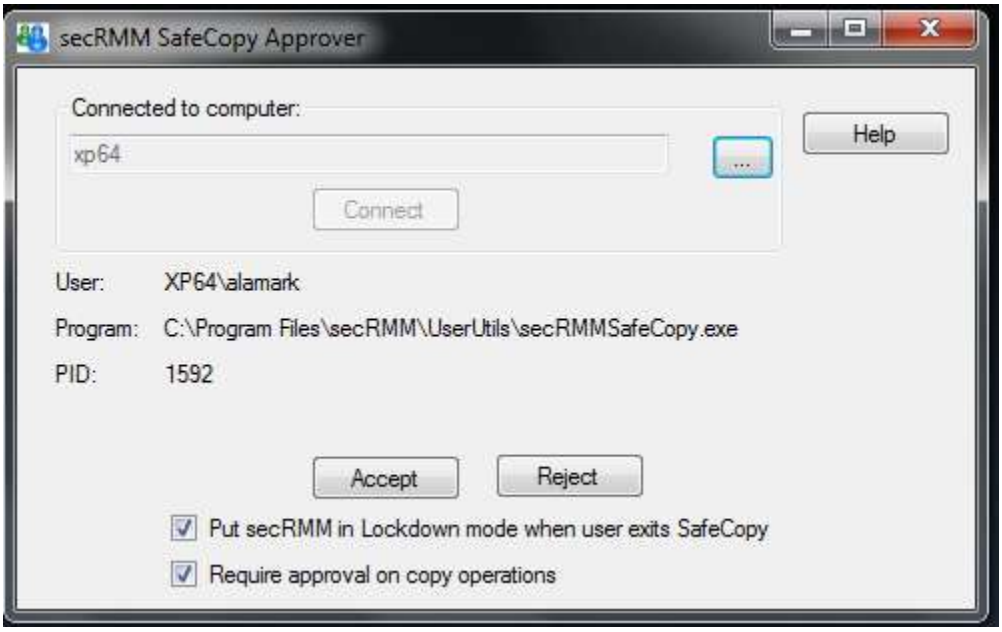


Figure 40 - Dialog to perform the approval, after connecting

Once connected, you will see the end-users UserId, the full path of the SafeCopy executable and the SafeCopy PID. If these values are consistent with the end-users environment, you can approve the request. You may also reject the request. You may also select to put secRMM into Lockdown mode once the end-user finishes using SafeCopy. You may also select to require that the end-users copy operations will need to be preapproved as well. If you require approval on copy operations, the

secRMMSafeCopyApprover program will show you the files and directories the user has selected to copy to a removable media device. You will have the option to accept or reject the end-users copy operation.

Firewall rule for secRMM SafeCopy Approver

One scenario for using the secRMM SafeCopy Approver program is to simply RDP (remote desktop) to the computer where the end-user is requesting approval. You can also perform the approval over the network. If you will use the secRMM SafeCopy Approver program on a remote computer (i.e. over the network) from where the end-user is requesting approval, you must enable an inbound firewall rule on the end-user computer(s). The rule is an inbound rule for TCP port 38865 (see screenshots below).

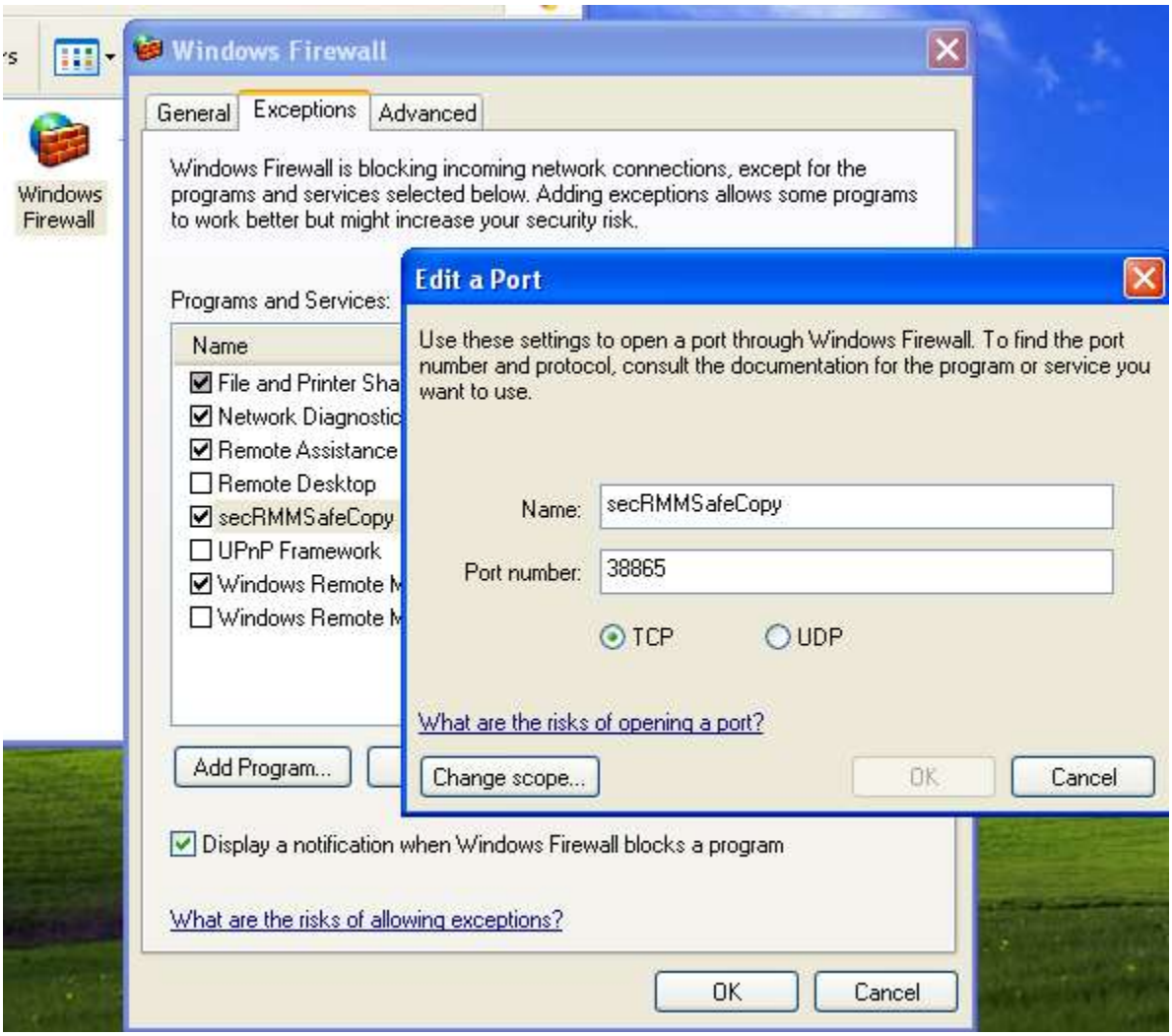


Figure 41 - secRMM SafeCopy Approver program firewall rule on Windows XP

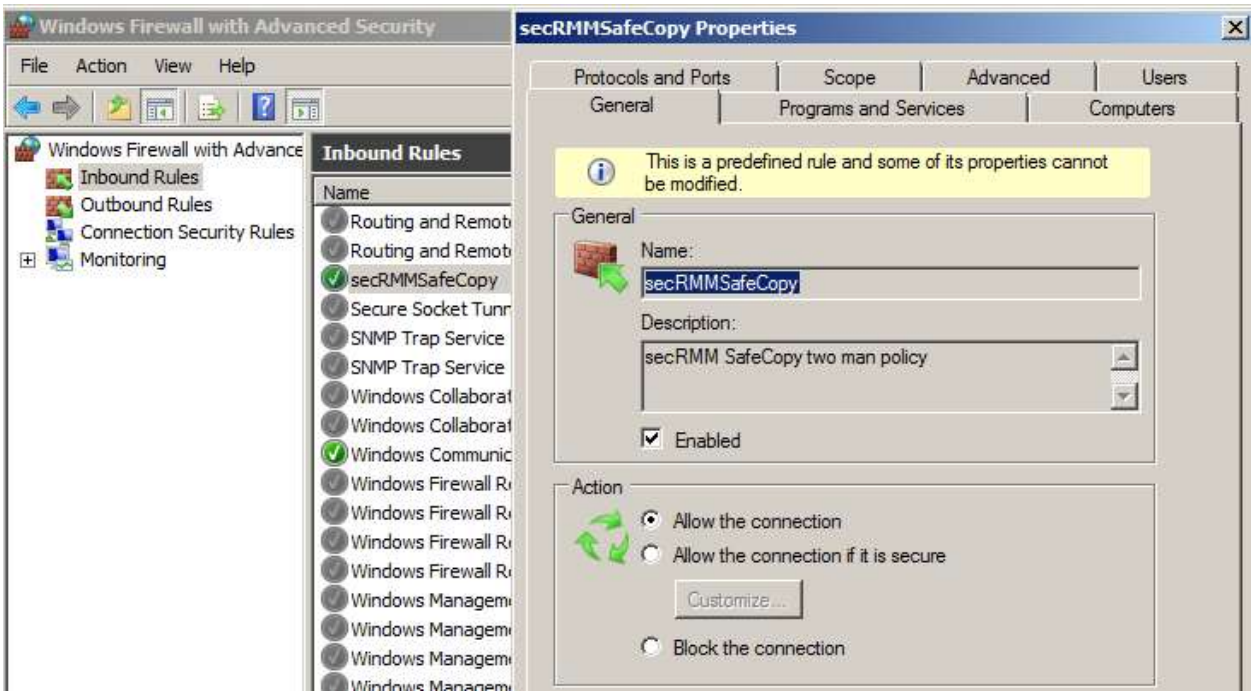


Figure 42 - secRMM SafeCopy Approver program firewall rule on Windows non-XP (i.e. advanced firewall)

Giving other users and/or groups permission to use the secRMM SafeCopy Approver program

You can give other users and/or groups the authority to approve the use of SafeCopy (i.e. use the secRMM SafeCopy Approver program). This frees the true IT Administrators (who have this permission by default) from having to perform the approval. To give other users and/or groups the authority to approve, in Windows Explorer, right mouse click on the secRMMSafeCopyApprover program (which is in the AdminUtils subfolder) and select Properties.

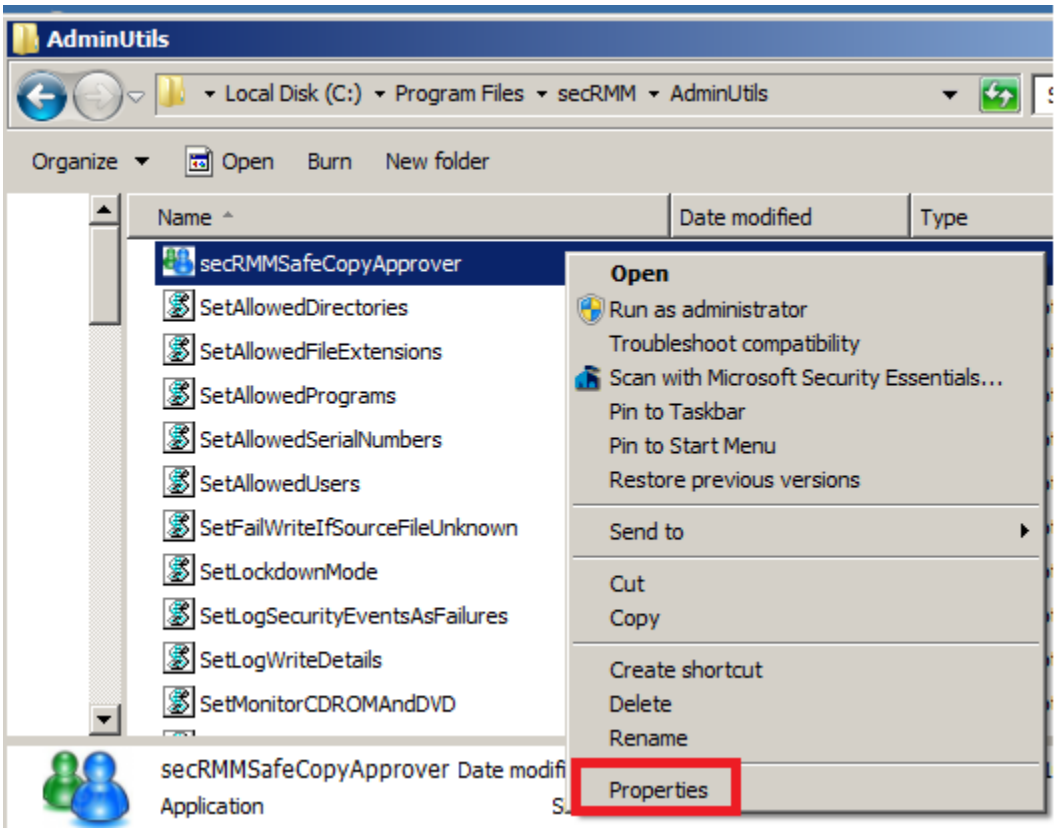


Figure 43 - secRMMSafeCopyApprover Properties

In the Properties dialog, select the Security tab and then click the Edit button. When you click the Edit button, the Permissions dialog will open. In the Permissions dialog, add the users and/or groups that you want to allow to use the secRMM SafeCopy Approver program. For each user and/or group you add, give them "Read & Execute" and "Read" permission. In the screenshot below, we are allowing User1.

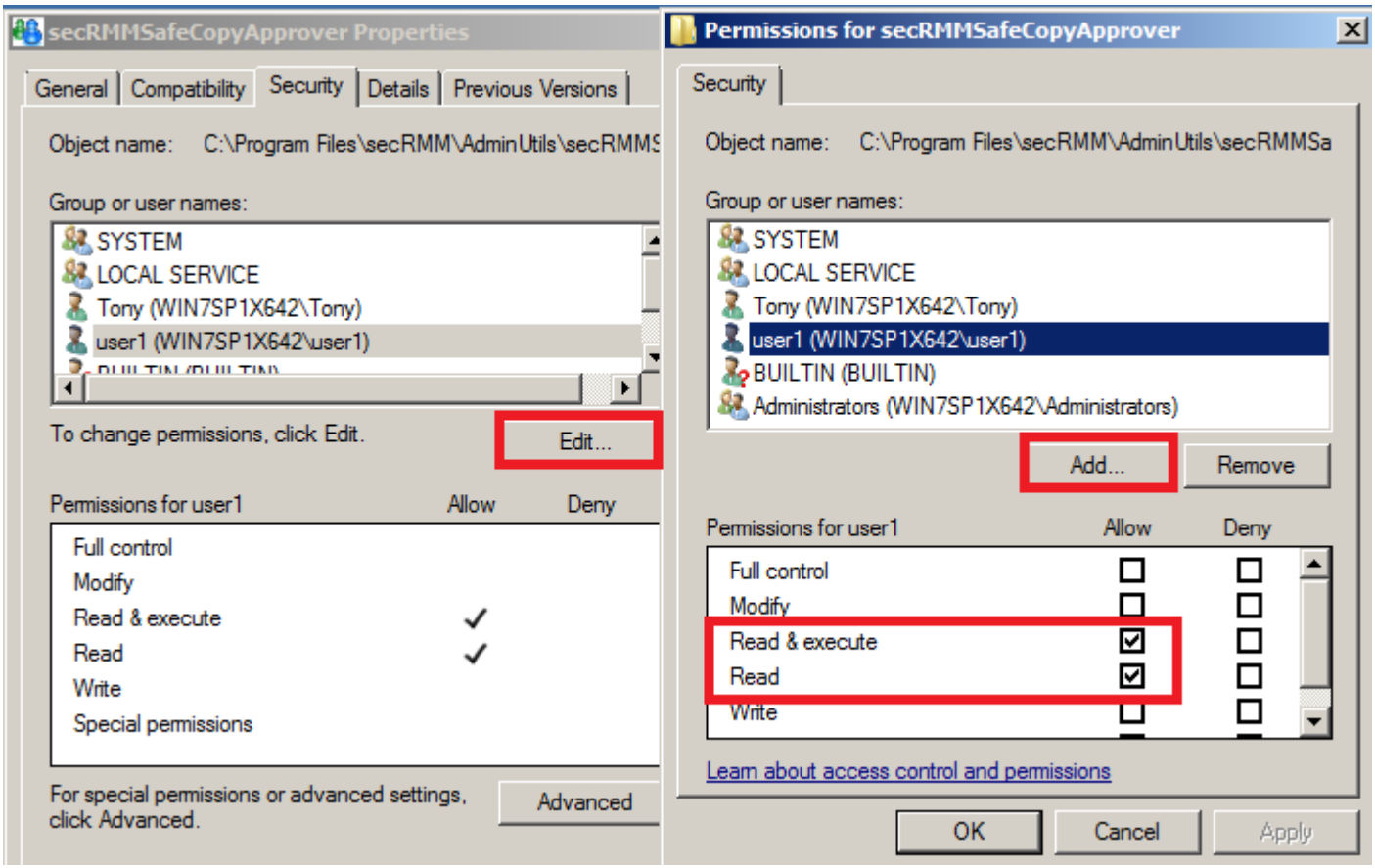


Figure 44 - secRMM SafeCopy Approver Permissions

Lastly, you can create a shortcut on the desktop for the secRMM SafeCopy Approver program. To do this, have the user(s) (who you added in the steps above) run the VBscript named CreateDesktopShortcutForSafeCopyApprover.vbs. This script is in the secRMMDeployment.zip (in the Miscellaneous directory) which you can download from the Squadra Technologies web site.

Licensing

secRMM has 4 flexible license modes:

1. Forest – All secRMM features are enabled.
2. Domain – All secRMM features are enabled.
3. Computer – All secRMM features are enabled.
4. Freeware – Only online and offline events are enabled. The authorization module and write events are disabled.

The table below lists the advantages and disadvantages of each license mode.

secRMM license type	Advantage	Disadvantage

Forest	Unlimited license for your Active Directory forest. Same license file for all computers in the forest.	
Domain	Unlimited license for your Active Directory domain. Same license file for all computers in the domain.	
Computer	Cost for small environments.	One license file per computer.
Freeware	Cost	All secRMM features are not available.

License Type

Forest license

Every Windows computer that runs secRMM will need a secRMM forest license file. The forest license file name will be the name of your forest with a file extension of lic. For example, if your forest is named contosoF.com, the secRMM forest license file would be named contosoF.com.lic. The secRMM forest license file needs to reside in the secRMM installation directory (by default, \Program Files\secRMM). To obtain the secRMM forest license file, you must contact Squadra Technologies.

The high-level sequence of events for secRMM forest licensing is summarized below:

1. Email your forest name to Squadra Technologies. In the AdminUtils subfolder, you can run the CMD program GetSecRMMLicenseInfo.exe to get your forest name.
2. Squadra Technologies will email back to you a secRMM forest license file.
3. The forest license file gets copied into the secRMM installation directory on each computer with secRMM installed on it.

Domain license

Every Windows computer that runs secRMM will need a secRMM domain license file. The domain license file name will be the name of your domain with a file extension of lic. For example, if your domain is named contoso.com, the secRMM domain license file would be named contoso.com.lic. The secRMM domain license file needs to reside in the secRMM installation directory (by default, \Program Files\secRMM). To obtain the secRMM domain license file, you must contact Squadra Technologies.

The high-level sequence of events for secRMM domain licensing is summarized below:

4. Email your domain name to Squadra Technologies. In the AdminUtils subfolder, you can run the CMD program GetSecRMMLicenseInfo.exe to get your domain name.
5. Squadra Technologies will email back to you a secRMM domain license file.
6. The domain license file gets copied into the secRMM installation directory on each computer with secRMM installed on it.

Computer license

Every Windows computer that runs secRMM will need a secRMM computer license file. The computer license file name will be the name of the Windows computer with a file extension of lic. For example, if there was a Windows computer named AcctingWrkSta1, the secRMM computer license file would be named AcctingWrkSta1.lic. The secRMM computer license file needs to reside in the secRMM installation directory (by default, \Program Files\secRMM). To obtain the secRMM computer license files, you must contact Squadra Technologies.

Creating the list of computers

Manual

To get the name of the computer, you can echo the COMPUTERNAME environment variable. To do this, open a command window and type:

echo %COMPUTERNAME%

Collect all the names of the computers in your environment using the method above. Email this list to Squadra Technologies.

Automated

If you are in a domain environment, you can run the VBscript named ListComputersInDomain.vbs. This script is in the secRMMDeployment.zip (in the Licensing\GatherInformation directory) which you can download from the Squadra Technologies web site. This script generates a list of computers from your Active Directory repository. Be sure you read the comment header in ListComputersInDomain.vbs as you will need to change the domain name to be your domain name (on line 36). To run the script, open an elevated command window and type:

cscript //NoLogo ListComputersInDomain.vbs > MyComputers.txt

The output of this script (in the example above, it will be the file MyComputers.txt) is what you will email to Squadra Technologies (see step 1 directly below).

The high-level sequence of events for secRMM computer licensing is summarized below:

1. Generate a list of all the computers in your environment that run secRMM.
2. Email the list generated in step 1 above to Squadra Technologies.
3. Squadra Technologies will email back to you a computer license file for every computer in the list.
4. The computer license file gets copied into the secRMM installation directory on each computer with secRMM installed on it.

Freeware license

Every Windows computer that runs secRMM will need a freeware license file. The freeware license file name will be FREEWARE.lic. The secRMM freeware license file needs to reside in the secRMM installation directory (by default, \Program Files\secRMM). To obtain the secRMM freeware license file, you must contact Squadra Technologies.

The high-level sequence of events for secRMM freeware licensing is summarized below:

1. Email your domain name to Squadra Technologies. In the AdminUtils subfolder, you can run the CMD program GetSecRMMLicenseInfo.exe to get your domain name.
2. Squadra Technologies will email back to you a freeware license file.
3. The freeware license file gets copied into the secRMM installation directory on each computer with secRMM installed on it.

Deploying the license

If you are in a workgroup environment (i.e. no domain) or you are doing a small deployment of secRMM, you can follow the "Small deployment" section below. If you are in a domain environment and/or have a large number of systems you want to deploy secRMM onto, please follow the section below titled "Large deployment".

Small deployment

You can use Windows Explorer or a command window to create a network share to the computer where secRMM is installed. Once you have created the network share, copy the secRMM license you received from Squadra Technologies to the secRMM installation directory (by default, \Program Files\secRMM).

Large deployment

The sections below describe options on how to distribute the secRMM license file(s).

GPO

You can distribute the secRMM license file with the Active Directory Group Policy Files feature. This is in the GPO Editor under [Computer Configuration|User Configuration]->Preferences->Windows Settings. It is a convenient method because you will receive a domain license from Squadra Technologies which is a single file that needs to be copied to the secRMM installation directory on each computer in your domain running secRMM. The Active Directory Group Policy Files feature is exactly intended to perform this task.

SCCM

You can distribute the secRMM license file with the System Center Configuration Manager Application Deployment (using a Script Deployment type) feature. secRMM has a separate **secRMM SCCM Installation Guide** document. You should reference that document for details.

Using a network share

This section describes a push technology utilizing Windows network shares.

1. Forest or domain license: Use the VBScript named DistributeSecRMM**Enterprise**LicenseViaNetworkShare.vbs
2. Computer license: Use the VBScript named DistributeSecRMM**Computer**LicenseViaNetworkShare.vbs
3. Freeware license: Use the VBScript named DistributeSecRMM**Freeware**LicenseViaNetworkShare.vbs

The VBScript file can be used to push the license files out to each computer running secRMM. This script is in the secRMMDeployment.zip (in the Licensing\Distribution directory) which you can download from the Squadra Technologies web site. You need to change line 20 of the script (i.e. the directory named

"C:\secRMM\Licenses\" to be the name of the directory where you put the secRMM license(s) (which you received from Squadra Technologies). To run the script, you will need domain admin privileges.

To run the script, open an elevated command window and type:

For Forest or domain license:
cscript DistributeSecRMM**Enterprise**LicenseViaNetworkShare.vbs MyComputers.txt

For Computer license:
cscript DistributeSecRMM**Computer**LicenseViaNetworkShare.vbs

For Freeware license:
cscript DistributeSecRMM**Freeware**LicenseViaNetworkShare.vbs MyComputers.txt

Creating the list of computers

Notice that the forest/domain and freeware licenses require an input file (in the example above, it is named MyComputers.txt). This text file contains the list of computers that you want to deploy the secRMM license to. Each line in the file is the name of a computer. If you are in a domain environment, you can run the VBscript named ListComputersInDomain.vbs. This script is in the secRMMDeployment.zip (in the Licensing\GatherInformation directory) which you can download from the Squadra Technologies web site. This script generates a list of computers from your Active Directory repository. Be sure you read the comment header in ListComputersInDomain.vbs as you will need to change the domain name to be your domain name (on line 36). To run the script, open an elevated command window and type:

cscript //NoLogo ListComputersInDomain.vbs > MyComputers.txt

Using a logon script

This section describes a pull technology utilizing Active Directory GPO computer or user logon scripts. Once you get the license file(s) from Squadra Technologies, put it/them into a shared directory (i.e. a share that is readable from every computer that has secRMM installed) so the secRMM license file(s) can be distributed.

1. Forest or domain license: Use the batch script named DistributeSecRMMEnterpriseLicenseViaLogonScript.cmd
2. Computer license: Use the batch script named DistributeSecRMMComputerLicenseViaLogonScript.cmd
3. Freeware license: Use the batch script named DistributeSecRMMFreewareLicenseViaLogonScript.cmd

The Batch script file can be integrated into an Active Directory GPO "computer startup" or "user logon" script to distribute the secRMM license files. This script is in the secRMMDeployment.zip (in the Licensing\Distribution directory) which you can download from the Squadra Technologies web site. You need to change line 3 of the script (i.e. the net use x: command) to match the shared directory that you put the secRMM license files in.

For "computer startup" scripts, in the Group Policy Management Editor, go to "Group Policy object"/Computer Configuration/Policies/Windows Settings/Scripts (Startup/Shutdown). Right click the

Startup Script (in the detail pane on the right) and specify the Batch script. Note that you should copy the Batch script file to a network share that is accessible by all the computers running secRMM.

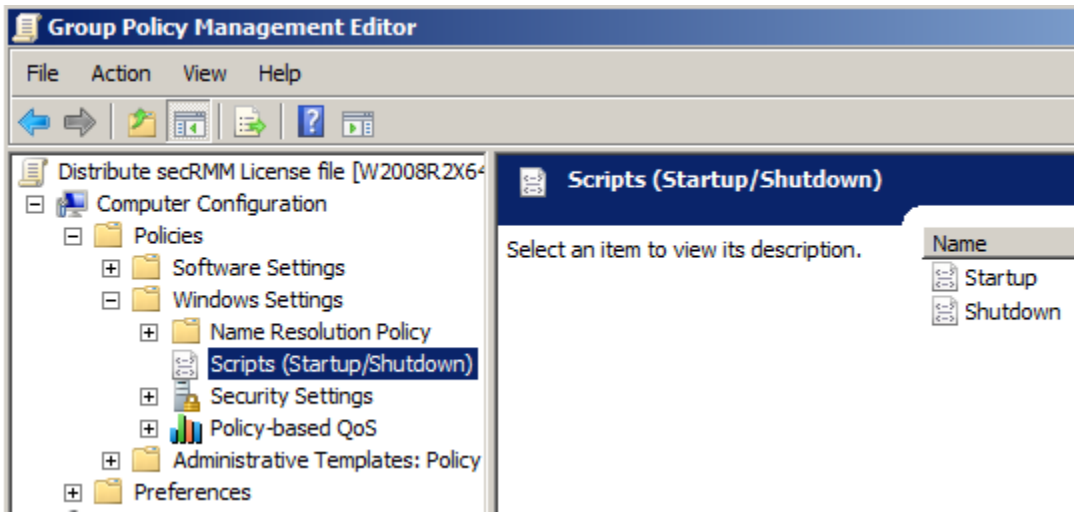


Figure 45 - AD GPO for Startup Script

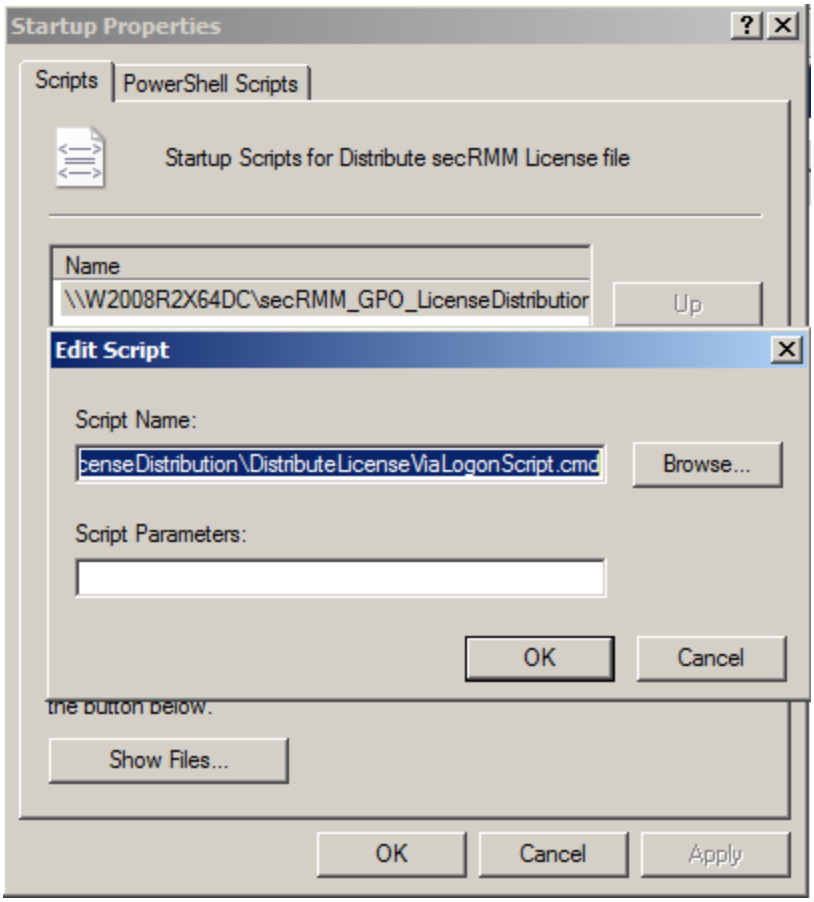


Figure 46 - Specify the Startup Script using a network share

For "user logon" scripts, in the Group Policy Management Editor, go to "Group Policy object"/User Configuration/Policies/Windows Settings/Scripts (Logon/Logoff). The steps will be the same as described above.

Managing the secRMM Event Log

Automatic backups

The secRMM event log is configured at installation to automatically backup when it becomes full. This guarantees that you will not lose events when the log becomes full since the Windows operating system will make a backup automatically and then clear the log so new events can be added. The default size of the secRMM event log is 1MB. The Windows default event log directory is C:\Windows\System32\winevt\Logs. The secRMM backup files will have the format Archive-secRMM-YYYY-MM-DD-HH-MM-SS-mmm.evtx. You should define a scheduled task for moving the backup files to another location (for example on a network drive). There is a Batch script named MoveRolledSecRMMEventLogs.cmd in the AdminUtils subfolder that moves the secRMM backup files from C:\Windows\System32\winevt\Logs to another location (by default, it moves them to C:\Program Files\secRMM\secRMMEventLogBackups).
While the automatic backup policy for secRMM is useful, your environment may have different policies in place for backing up security data such as the data collected by secRMM. If this is the case, please read the subsection below.

Scheduled task backups

If your environment has an event log backup policy and you want more control over the backup policy for the secRMM event log, the secRMM product ships a Batch script (named BackupSecRMMEventLog.cmd) that will backup and then clear the secRMM event log. BackupSecRMMEventLog.cmd is located in the AdminUtils subfolder.

If you want to use BackupSecRMMEventLog.cmd, you can set a scheduled task on each system running secRMM that calls BackupSecRMMEventLog.cmd. The frequency of running the scheduled task will be based on how often you anticipate a removable media device being used and how large you make the secRMM event log. Make sure that the scheduled task runs in administrator mode (or as the SYSTEM account) since access to the secRMM event log requires this elevated administrative state. When you create the scheduled task, be sure to check the checkbox labeled "Run with highest privileges" on the General tab.

Backing up locally

By default, the backed up secRMM event log files generated by BackupSecRMMEventLog.cmd will go into the secRMMEventLogBackups subfolder under the secRMM product directory (by default, this will be \Program Files\secRMM) so the complete backup directory will be \Program Files\secRMM\ secRMMEventLogBackups.

Backing up to network

You can make BackupSecRMMEventLog.cmd backup to a network share by changing line 24 of the script. This line defines a script variable named ARCHIVEtoNETWORK. Two examples of how you might change the line are shown below:

```
SET ARCHIVEtoNETWORK=\\COMPUTERNAME\C$\Archives\secRMM
or
SET ARCHIVEtoNETWORK=x:\Archives\secRMM
```

The next section explains how you can use Active Directory Group Policy Objects to schedule this task.

Active Directory Deployment

You can use Active Directory (AD) Group Policy Objects (GPO) to create the scheduled task. In the Group Policy Management Editor, go to "Group Policy object"/Computer Configuration/Preferences/Control Panel Settings/Scheduled Tasks.

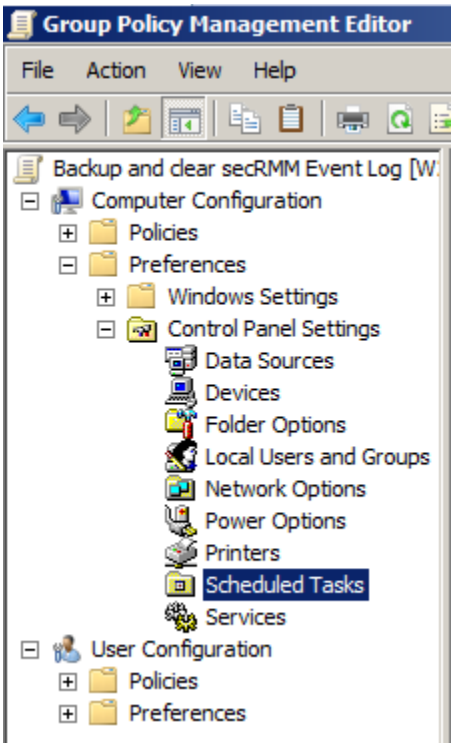


Figure 47 - AD GPO for Scheduled Task

Right-click the Scheduled Tasks node, point to New, and select Scheduled Task.

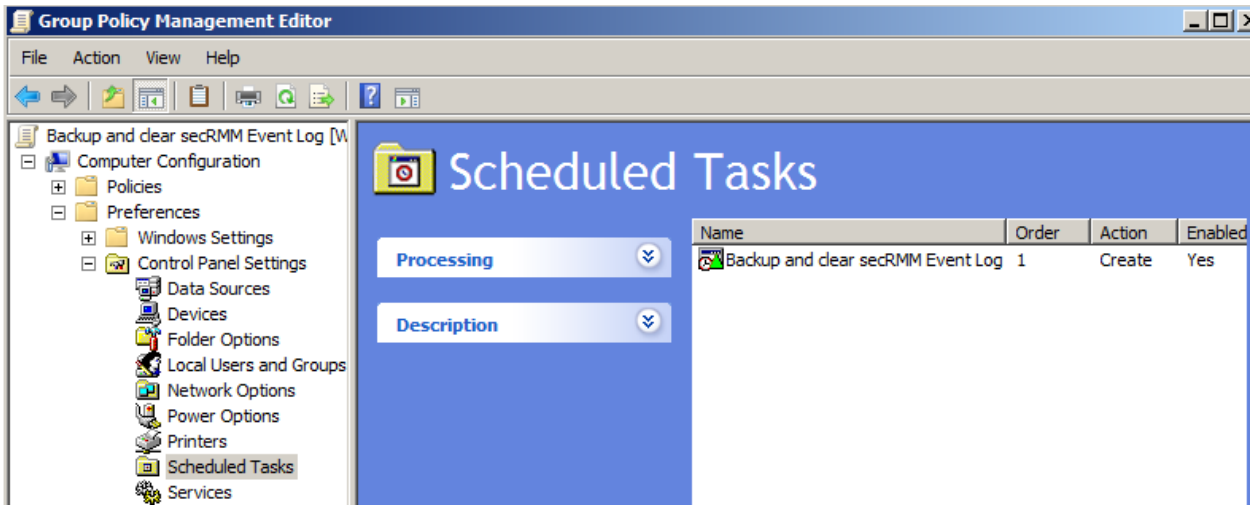


Figure 48 - Creating the AD GPO Scheduled Task

On the Task tab, in the Action drop-down, select Create. Give the scheduled task a name (ex: Backup and clear secRMM Event Log). In the Run field, put C:\Program Files\secRMM\AdminUtils\BackupSecRMMEventLog.cmd (make sure this directory is where you installed secRMM). The arguments, start in and comments fields are optional. For user name and password specify a userid that is an Administrator.

On the Schedule tab, specify when and how often you want to run this task.

On the Settings and Common tabs, specify any properties here that you want to apply to your environment.

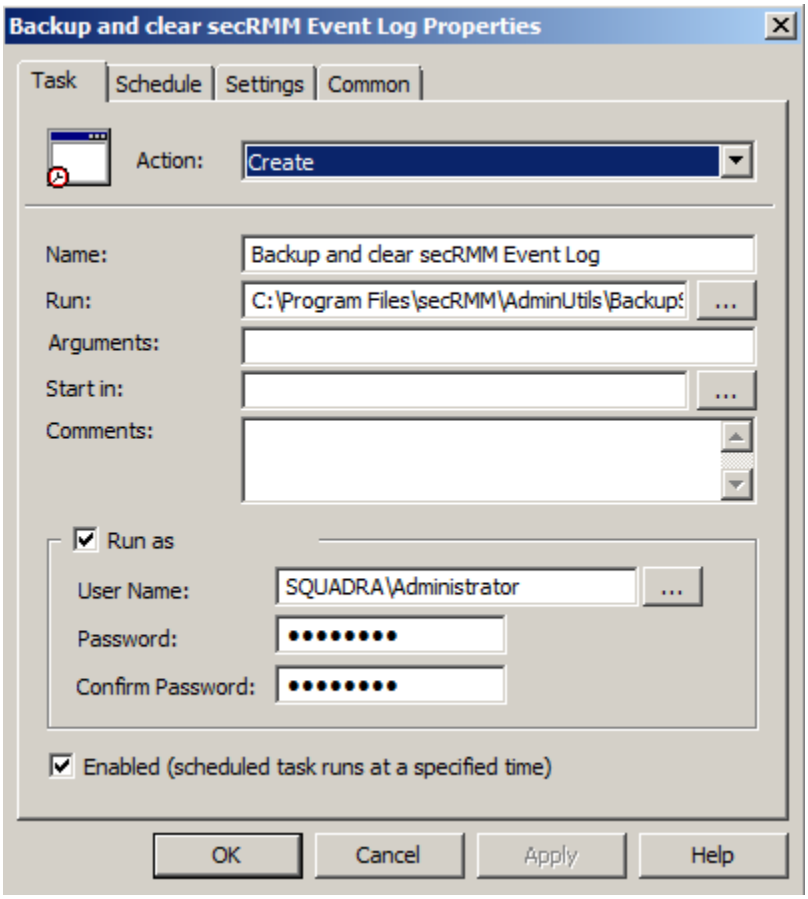


Figure 49 - AD GPO Scheduled Task Properties

There is also a CMD script/snippet named UserLoginScriptToBackupToNetworkShare.cmd in the AdminUtils subfolder. You can use this as a baseline to integrate scheduling tasks from a user login script.

Integrating secRMM data into your environment

The secRMM product is intended to run silently in the background. However, it is generating security events that should be taken seriously. To that end, you should consider integrating the secRMM events that are being generated into your company's security/monitoring strategy/implementation. There are many enterprise management products on the market today. Some of the more popular products are: Microsoft System Center (Operations Manager (SCOM), Configuration Manager (SCCM) and Orchestrator), Splunk, CA UniCenter, IBM Tivoli and Director, HP OpenView, Nagios, SolarWinds, to name a few. All of these types of products are capable of:

1. pulling events from the Windows event logs and/or
2. consuming WMI events and/or
3. receiving SNMP traps

secRMM generates all 3 of the methods listed above.

In addition to writing to the Windows event logs, secRMM is also generating its own WMI events. For every secRMM Windows event you see in the Windows event logs, secRMM has generated a corresponding

secRMM WMI event. These secRMM events can be consumed by any program or script. WMI provides a very elegant model which Microsoft calls the producer/consumer model where secRMM is the producer (of security events) and another program(s) can consume the secRMM events in real time. If you are familiar with SNMP, it is similar to a SNMP trap. With this background in mind, you can further integrate the information that secRMM generates to perform many security related automation tasks. Please feel free to contact Squadra Technologies for help on this integration technology. The possibilities are limitless!

secRMM is also capable of generating SNMP traps (or informs). secRMM supports SNMP versions 1, 2 and 3. For details on how to configure secRMM for SNMP, please see the section below titled SNMP.

Microsoft System Center

secRMM System Center documentation can be found at http://www.squadratechnologies.com/Products/secRMM/SystemCenter/secRMMSystemCenter.aspx.

SNMP

The secRMM SNMP dialog below is available from the secRMM MMC. It is also accessible from the secRMM Excel 2010 AddIn. You can also control secRMM SNMP from the SetSNMP.vbs script in the AdminUtils subfolder. The SNMP values you must provide are dependent on your SNMP environment. If you do not know what these values should be, you will need to ask the SNMP system administrators in your environment. Be sure you check the "Enable" checkbox once you have confirmed that the SNMP values are correct.

secRMM has a SNMP MIB file (the actual file name is secRMMSNMP-MIB.txt) available on the Squadra Technologies web site. SNMP MIB files are used by the management station(s) receiving the traps from secRMM. While SNMP MIB files are not absolutely required, they are useful to the SNMP system administrators who may be writing trap handlers or just want to see more descriptive text (instead of raw SNMP OIDs).

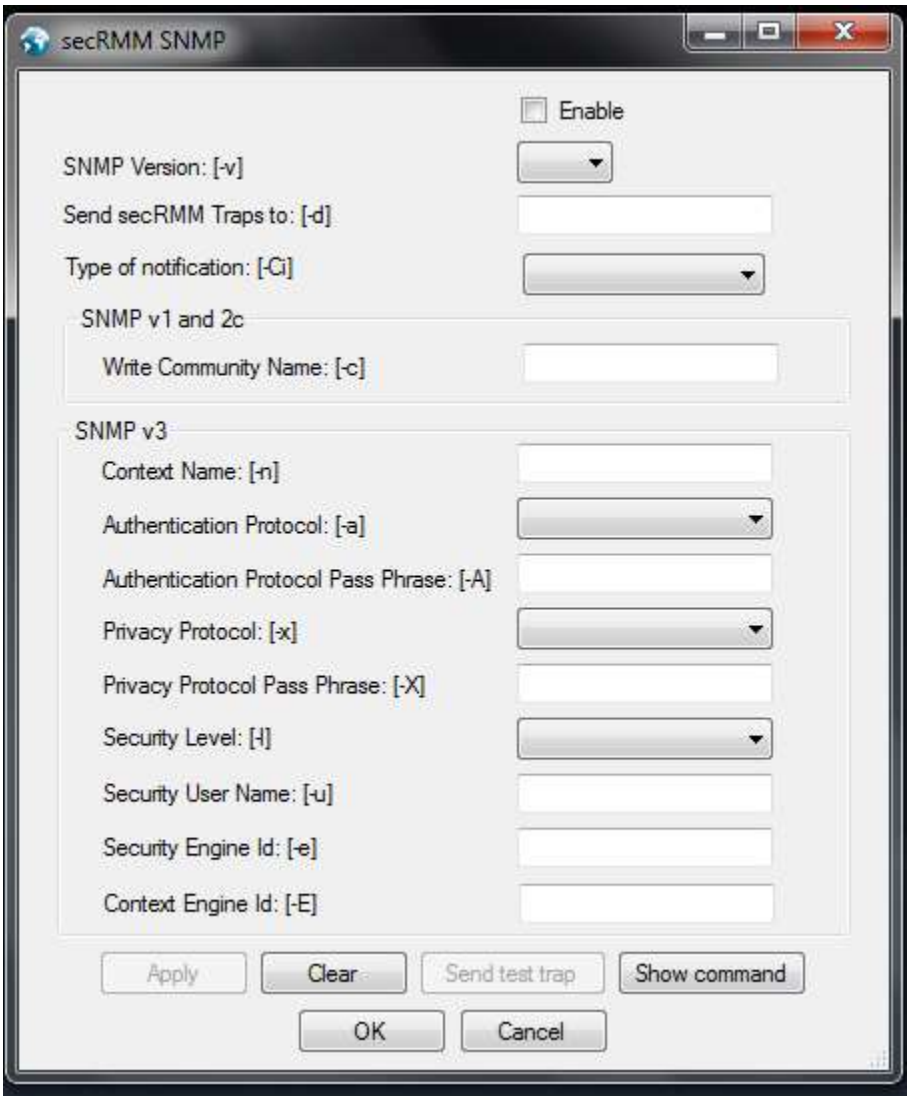


Figure 50 - secRMM SNMP dialog

Event Forwarding

If you would like to forward the secRMM events to another enterprise management framework, the event information below will help you with the integration process.

```
EventId 400: online event, secRMM_MESSAGE_400
- Occurs when a plug-and-play storage device is attached to the Windows computer, including mobile
devices.

EventId 401: write started event secRMM_MESSAGE_401
- Occurs when a file copy operation begins.  This event is seldom used and only clutters up the event
log.

EventId 402: write completed event secRMM_MESSAGE_402
- Occurs when a file copy operation completes.

EventId 403: offline event, secRMM_MESSAGE_403
```

- Occurs when a plug-and-play storage device is removed from the Windows computer, including mobile devices.

EventId 500: UserAuthorizationFailedEvent secRMM_MESSAGE_500
- Occurs when a user who is not in the secRMM AllowedUsers list attempts to perform a file copy operation to a removable storage device.

EventId 501: ProgramUsedAuthorizationFailedEvent secRMM_MESSAGE_501
- Occurs when a program that is not in the secRMM AllowedPrograms list attempts to perform a file copy operation to a removable storage device.

EventId 502: SerialNumberUsedAuthorizationFailedEvent secRMM_MESSAGE_502
- Occurs when a file copy operation is attempted to a removable storage device that is not in the secRMM AllowedSerialNumbers list.

EventId 503: UnknownSourceFailedEvent secRMM_MESSAGE_503
- Occurs when a file copy operation is attempted to a removable storage device and secRMM cannot determine the source file name of the file being copied.
- The most common reason for this event is when a user tries to save a file directly to the removable storage device.

EventId 504: SourceDirectoryFailedEvent secRMM_MESSAGE_504
- Occurs when a file copy operation is attempted to a removable storage device from a directory that is not in the secRMM AllowedDirectories list.

EventId 505: SourceFileExtensionFailedEvent secRMM_MESSAGE_505
- Occurs when a file copy operation is attempted to a removable storage device for a file whose file extension is not in the secRMM AllowedFileExtensions list.

EventId 506: InternalIdUsedFailedEvent secRMM_MESSAGE_506
- Occurs when a file copy operation is attempted to a removable storage device whose internal id (VID/PID) is not in the secRMM AllowedInternalIds list.

EventId 507: SerialNumberUsedAuthorizationFailedEventOnline secRMM_MESSAGE_507
- Occurs when a removable storage device that is not in the secRMM AllowedSerialNumbers list is attached to the Windows computer. The [EnforceWhenPluggedIn] prefix is specified on the secRMM AllowedSerialNumbers property.
- The removable storage device is unmounted from the Windows system.

EventId 508: InternalIdUsedFailedEventOnline secRMM_MESSAGE_508
- Occurs when a removable storage device whose internal id (VID/PID) is not in the secRMM AllowedInternalIds list is attached to the Windows computer. The [EnforceWhenPluggedIn] prefix is specified on the secRMM AllowedInternalIds property.
- The removable storage device is unmounted from the Windows system.

EventId 509: UserAuthorizationFailedEventOnline secRMM_MESSAGE_509
- Occurs when a user who is not in the secRMM AllowedUsers list is logged into the Windows computer when a removable storage device is attached to the Windows computer. The [EnforceWhenPluggedIn] prefix is specified on the secRMM AllowedUsers property.
- The removable storage device is unmounted from the Windows system.

EventId 510: BlockCdDvdWritesEventOnline secRMM_MESSAGE_510
- Occurs when a Cd/Dvd is inserted into the Windows computer and the secRMM BlockCDROMAndDVDWrites property is on (checked). The [EnforceWhenPluggedIn] prefix is specified on the secRMM BlockCDROMAndDVDWrites property.
- The Cd/Dvd is unmounted from the Windows system.

EventId 511: BlockCdDvdWritesEventOnline secRMM_MESSAGE_511
- Occurs when a file copy operation is attempted to a Cd/Dvd disc and the secRMM BlockCDROMAndDVDWrites property is on (checked).

EventId 512: AllowBitLockerOnlyEventOnline secRMM_MESSAGE_512
- Occurs when a removable storage device that is not BitLocker protected is attached to the Windows computer and the secRMM AllowBitLockerOnly property is on (checked). The [EnforceWhenPluggedIn] prefix is specified on the secRMM AllowBitLockerOnly property.
- The removable storage device is unmounted from the Windows system.

EventId 513: AllowBitLockerOnlyEvent secRMM_MESSAGE_513
- Occurs when a file copy operation is attempted to a removable storage device that is not BitLocker protected and the secRMM BlockCDROMAndDVDWrites property is on (checked).

EventId 514: BlockProgramsOnDevice secRMM_MESSAGE_514
- Occurs when an attempt is made to execute a program that resides on the removable storage device and the secRMM BlockProgramsOnDevice property is on (checked).

EventId 515: AllowRMSFilesOnly secRMM_MESSAGE_515
- Occurs when a file copy operation is attempted for a file that is not protected by Microsoft Rights Management Services (RMS) and the secRMM AllowRMSFilesOnly property is on (checked).

EventId 600: Trial Mode (Licensing)
- Occurs when the secRMM software is running in trial mode and a plug-and-play storage device is attached to the Windows computer, including mobile devices.

EventId 601: Invalid License (Licensing)
- Occurs when the secRMM software does not have a valid license file and a plug-and-play storage device is attached to the Windows computer, including mobile devices.

EventId 300-309: External
- Occurs when an external secRMM event occurs (ex: clear the secRMM log, backup the secRMM log, etc.).
- These event ids are available to IT/system administrators to add custom removable storage events to the secRMM event log

EventId 700: Property Change secRMM_MESSAGE_700
- Occurs when a secRMM property changes.

EventId 800:
- Occurs when the secRMM SafeCopy program starts.

EventId 801:
- Occurs when the secRMM SafeCopy program is requesting approval to use. The secRMM PreApproveSafeCopy property is on (checked).

EventId 802:
- Occurs when the secRMM SafeCopy program is requesting approval to use and an administrator has approved the SafeCopy session. The secRMM PreApproveSafeCopy property is on (checked).

EventId 803: SafeCopy error
- Occurs when the secRMM SafeCopy program is requesting approval to use and an administrator has rejected the SafeCopy session. The secRMM PreApproveSafeCopy property is on (checked).
- SafeCopy terminates after the end-user closes the rejection notice dialog.

EventId 804: SafeCopy error
- Occurs when the secRMM SafeCopy program is requesting approval to use and the end-user clicks the cancel button. The secRMM PreApproveSafeCopy property is on (checked).

```
- SafeCopy terminates when the end-user clicks the cancel button.

EventId 805:
- Occurs when the secRMM SafeCopy program copys a file to a removable storage device.

EventId 806:
- Occurs when the secRMM SafeCopy program deletes a file from a removable storage device.

EventId 807:
- Occurs when the secRMM SafeCopy program creates a folder (directory) on a removable storage device.

EventId 808:
- Occurs when the end-user maps a network drive/share within the secRMM SafeCopy program.

EventId 809: SafeCopy error
- Occurs when the secRMM SafeCopy program terminates.

EventId 810: SafeCopy error
- Occurs when the end-user cancels a copy operation within the secRMM SafeCopy program.

EventId 811: SafeCopy error
- Occurs when a copy operation fails within the secRMM SafeCopy program.

EventId 812: SafeCopy error
- Occurs when a second instance of the secRMM SafeCopy program attempts to start.  Only one instance of
the secRMM SafeCopy program is allowed.

EventId 813: SafeCopy error
- Occurs when secRMM is not properly installed on the Windows computer and the secRMM SafeCopy program
is started.
```

Known issues

1. XP does not allow putting access control on event logs (i.e. the CustomSD property). This means your end users can view the secRMM event log. However, they CANNOT clear the log. In addition, the description text (for the end users) is not formatted properly.
2. On XP and W2003, when a user performs an Explorer "cut and paste" (i.e. a file move operation) to a Removable Media Device, secRMM cannot determine the source file(s). The "copy" to a Removable Media Device is not affected however.
3. Based on how the network share is mapped, copying zip files over the network to a WPD device (i.e. a removable media device that does not have a drive letter assigned to it) will not list the files contained within the zip as secRMM normally does.
4. Although Blackberry devices are supported in the secRMM 7.0.0.0 release, we are still working on fixing an issue. The issue is that SafeCopy will sometimes get into a state when the BB device is mounted where the device continues to toggle from online to offline. We are working to correct this issue.
5. Starting with IOS 8.3, Apple has unfortunately locked down the App data directories unless the App was built with the UIFileSharingEnabled flag set. secRMM SafeCopy has been modified to handle this.
6. The Azure/HyperV/RDP feature is currently not able to unmount the USB device within the remote connected computer (i.e. the RDP server). This limits the full functionality of secRMM on the

remote machine since the "eject on mount rules" will not remove the device as it does on physical computers. This is just an inconsistency, since the user will still not be able to access the virtual drive. We are working to correct this issue.

7. The Azure/HyperV/RDP feature does not yet support mobile devices. We will provide this functionality very soon.
8. The ScanDevice property does not yet support mobile devices. We are investigating on how to provide this functionality.

Contacting Squadra Technologies Support

Squadra Technologies Support is available to customers who have purchased a commercial version of secRMM and have a valid maintenance contract or who are in a trial mode of the product.

When you contact Support please include the following information:

1. The version of secRMM you have installed.
2. The Windows versions you have installed: XP, 2003 Server, 2008 Server R2, Vista, Windows 7, Windows 8, Windows 10 etc.
3. Whether the Windows Operating System is 32bit or 64bit.
4. The specific issue you are contacting support for.

About Squadra Technologies, LLC.

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

Contacting Squadra Technologies, LLC.

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