
secRMM

Security Removable Media Manager



secRMM Microsoft System Center Integration

Squadra Technologies is focused on providing System Center solutions to help organizations be more secure and productive. Squadra's secRMM is a Windows security product that tightly integrates into System Center to provide enterprise management policy rules to protect removable storage activities within the data center. By combining secRMM, Microsoft System Center and Microsoft BitLocker an organization will have complete security and control over their removable storage.

secRMM is Windows security software that audits and authorizes write activity to storage devices. This includes mobile (smart phones/tablets), flash drives (including hardware and/or software encryption), external hard drives, SD-Cards, and CD/DVD.

secRMM can act as a Data Loss Prevention (DLP) add-on to Microsoft System Center Endpoint Protection. Organizations that have in the past used third party antivirus solutions for DLP can now choose to use System Center Instead. secRMM completes Microsoft's endpoint protection strategy (antimalware, firewall, software updates) by adding DLP.



SCCM Console

Squadra Technologies
7575 West Washington Ave.
Suite 127-252
Las Vegas, NV 89128
+1 (562) 221-3079

For More Information Contact:
info@squadratechnologies.com

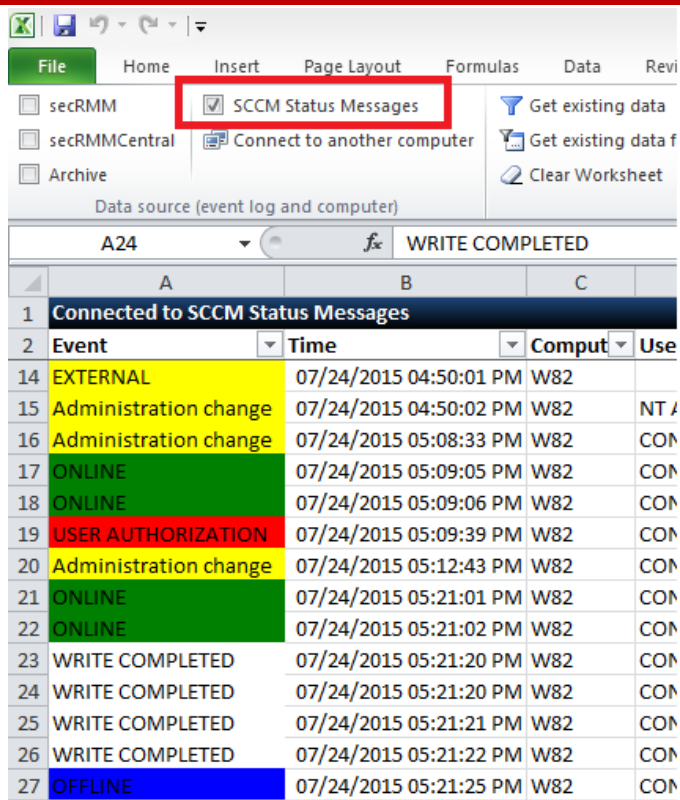
Free Trial Download Visit:
www.squadratechnologies.com

ENHANCED SCCM INTEGRATION secRMM v 7.0.

secRMM version 7.0 provides more integration points with Microsoft System Center Configuration Manager 2012 (SCCM). Prior to version 7.0, secRMM offered the SCCM Console Extension that allowed centralized policy management/configuration. The new enhanced secRMM features in version 7.0 tie in with the Console Extension and allow you to work with secRMM without ever having to leave the SCCM console!

secRMM v 7.0 SCCM Enhancements:

- secRMM SCCM Status Messages
- secRMM SCCM Reports
- secRMM Excel Add-In to View the SCCM Status Messages



	A	B	C	
1	Connected to SCCM Status Messages			
2	Event	Time	Comput	Use
14	EXTERNAL	07/24/2015 04:50:01 PM	W82	
15	Administration change	07/24/2015 04:50:02 PM	W82	NT /
16	Administration change	07/24/2015 05:08:33 PM	W82	CON
17	ONLINE	07/24/2015 05:09:05 PM	W82	CON
18	ONLINE	07/24/2015 05:09:06 PM	W82	CON
19	USER AUTHORIZATION	07/24/2015 05:09:39 PM	W82	CON
20	Administration change	07/24/2015 05:12:43 PM	W82	CON
21	ONLINE	07/24/2015 05:21:01 PM	W82	CON
22	ONLINE	07/24/2015 05:21:02 PM	W82	CON
23	WRITE COMPLETED	07/24/2015 05:21:20 PM	W82	CON
24	WRITE COMPLETED	07/24/2015 05:21:20 PM	W82	CON
25	WRITE COMPLETED	07/24/2015 05:21:21 PM	W82	CON
26	WRITE COMPLETED	07/24/2015 05:21:22 PM	W82	CON
27	OFFLINE	07/24/2015 05:21:25 PM	W82	CON

secRMM Excel Add-in

SCOM INTEGRATION. secRMM comes with a Microsoft System Center Operations Manager Management Pack (MP). This lets organizations to incorporate removable media events into their centralized console (i.e. Operations Manager console). Additionally, secRMM comes with Operations Manager data warehouse reporting and “Audit and Collection Services” (ACS) reporting. This allows organizations to set up alerts, notifications, tasks, reports, and can optionally generate SNMP trap, among other desirable capabilities

secRMM ACTS AS A FIREWALL. secRMM acts like a firewall between Windows and the removable storage devices by injecting a kernel mode device driver. This is advantageous because it prevents hackers from stopping secRMM from performing its functions. secRMM can take advantage of Microsoft Active Directory so that the secRMM authorization policies are tied to the user (i.e. user configuration/policy). Again, secRMM’s functionality is a great compliment to Microsoft System Center 2012 Endpoint Protection and Microsoft BitLocker.

EASY DEPLOYMENT VIA MICROSOFT SYSTEM CENTER CONFIGURATION MANAGER OR ACTIVE DIRECTORY.

secRMM can easily be deployed via Microsoft System Center Configuration Manager or Active Directory Group Policy because it’s architecture relies solely on the base Windows Operating System components. secRMM does not need its own framework. This makes secRMM particularly cost effective compared to other solutions. Furthermore, secRMM is completely functional within the Windows Event Log and the base Microsoft Management Console (“MMC”). Given these efficiencies Squadra is able to provide the software at *affordable pricing*.

CONFIGURATION. Configuration of secRMM can be performed using the SCCM Console, the local Computer Management Microsoft Management Console (MMC), Active Directory Group Policy Editor, a System Center Orchestrator workflow and/or any Microsoft scripting language.

Squadra Technologies
7575 West Washington Ave.
Suite 127-252
Las Vegas, NV 89128
+1 (562) 221-3079

For More Information Contact:
info@squadratechnologies.com

Free Trial Download Visit:
www.squadratechnologies.com