

Security Removable Media Manager OpenDxl Administrator Guide

Version 9.11.27.0 (April 2024) Protect your valuable data



© 2011 Squadra Technologies, LLC. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Squadra Technologies, LLC.

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

Squadra Technologies, LLC 4201 State Route W Cleveland, Missouri 64734 USA www.squadratechnologies.com email: info@squadratechnologies.com

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

TRADEMARKS

Squadra Technologies, secRMM are trademarks and registered trademarks of Squadra Technologies, LLC. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Disclaimer

The information in this document is provided in connection with Squadra Technologies products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Squadra Technologies products. EXCEPT AS SET FORTH IN Squadra Technologies's TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, Squadra Technologies ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL Squadra Technologies BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF Squadra Technologies HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Squadra Technologies makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Squadra Technologies does not make any commitment to update the information contained in this document.

Squadra Technologies Excel AddIn Administrator Guide Created - August 2011

Contents

INTRODUCTION	4
INSTALLATION OF SECRMM	4
Prerequisites for OpenDxL	5
Checking for an existing python install	5
Install python	6
Install the OpenDxl python client	10
CONFIGURE SECRMM TO SEND SECURITY EVENTS TO THE OPENDXL FABRIC/SERVERS	12
OpenDxl Configuration File	17
Data format and which secRMM events	21
CONFIGURE THE OPENDXL FABRIC/SERVERS TO RECEIVE SECRMM EVENTS	22
Send a test security event from secRMM to the OpenDxl fabric/servers	24
CONTACTING SQUADRA TECHNOLOGIES SUPPORT	25
ABOUT SQUADRA TECHNOLOGIES, LLC.	26

Introduction



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.

secRMM integrates into platforms/frameworks that support OpenDxl. secRMM generates very detailed security auding data (events) for removable storage devices (probably the best in the entire security industry). It is advantageous for security administrators and analysts to have a central place to view the secRMM security events in real time and as reports for post analysis.

OpenDxl is an initiative to create adaptive systems of interconnected services that communicate and share information for real-time, accurate security decisions and actions. You can read more about OpenDxl at the OpenDxl Home Page:

<u>https://www.opendxl.com/</u>. Open security initiatives will allow for the best security product to be integrated together because the collecting framework will speak a general language. You can read more about this concept at: <u>https://opencybersecurityalliance.org/</u>. One such product on the market today is McAfee/Trellix enterprise Policy Orchestrator (ePO for short). You can read more about ePO at: <u>https://www.trellix.com/products/epo/</u>.

NOTE: This document is 95% screenshots so don't get discouraged with the number of pages! Hopefully you will find that a picture is really worth 1000 words.

Installation of secRMM

secRMM is a standard/generic Windows installation file (i.e. a msi file). It has both a 64-bit and 32-bit installer. To get started integrating secRMM into your OpenDxl environment, you simply need to install the secRMM msi. secRMM is used in many enterprise environments and is being deployed using Microsoft Configuration Manager, Microsoft Intune, Microsoft Active Directory and other tools that support Windows msi file deployments. Based on your environment, please visit https://www.squadratechnologies.com/Products/secRMM/secRMMDocumentation.aspx to get the tool that is used in your environment. If you need help getting started, please email support@squadratechnologies.com and we would be happy to provide our free technical assistance over a screensharing session or a phone call if you cannot share your screen.

Once you have secRMM installed into the Windows endpoint computer, there will be a directory (which you need to be an Administrator to access) at:

C:\Program Files\secRMM\AdminUtils\OpenDxl. Note that you can override the default secRMM installation directory but C:\Program Files\secRMM is the default. The screenshot below shows the directory. These files are used by secRMM to send the secRMM security events to the OpenDxl fabric/servers.

📙 🛛 🛃 🚽 🛛 OpenDxI				
File Home Share View				
Pin to Quick Copy Paste shortcut	Move Copy to * Copy	New item •	Properties	it Select all
Clipboard	Organize	New	Open	Select
\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This PC \rightarrow OS (C:) \rightarrow	Program Files > secRMM > Ad	lminUtils → OpenDxI		
	^			e:
Name	D	ate modified	уре	Size
Cache	1/	/15/2024 1:25 PM F	ile folder	
📑 comm	on.py 12	2/8/2023 3:01 PM P	ython File	1 KB
📓 GetOp	enDxIClient.ps1 1/	/14/2024 3:54 PM V	Vindows PowerS	4 KB
Pythor	Path.txt 1/	/15/2024 6:09 AM T	ext Document	0 KB
secRM	MOpenDxI.cmd 12	2/8/2023 3:54 PM V	Vindows Comma	2 KB
🔊 secRM	MOpenDxI.ps1 1/	/15/2024 6:53 AM V	Vindows PowerS	27 KB
secRM	MOpenDxI.ps1.log 1/	/11/2024 12:12 PM L	.OG File	0 KB
📄 secRM	MOpenDxI.py 1/	/15/2024 5:25 AM P	ython File	9 KB
i secRM	MOpenDxI.py.log 1/	/11/2024 12:12 PM L	.OG File	0 KB
secRM	MOpenDxIDisable.cmd 1/	/11/2024 12:43 PM V	Vindows Comma	1 KB
secRM	MOpenDxlEnable.cmd 1/	/11/2024 12:43 PM V	Vindows Comma	1 KB

Prerequisites for OpenDxl

The prerequisites for using secRMM in an OpenDxl environment are:

- 1. The Windows computer where secRMM is running needs to have Python version 3.8 or 3.9 installed.
- 2. The OpenDxl python client needs to be installed.

Satisfying these 2 prerequisites are explained below.

Checking for an existing python install

Before downloading python, you may want to check to see if python is already installed in the Windows computer running secRMM. After all, if you are using an OpenDxl product in your environment, you probably have already configured your Windows endpoints. Luckily, on Windows, python installed an executable file into the C:\Windows directory called py.exe. Py.exe is the python launcher for Windows.

Open a command prompt window (running as administrator) and type: where py

As you can see in the screenshot below, the Windows operating system shows you that py.exe resides in C:\Windows\py.exe. The directory C:\Windows is a system directory and is always included in the PATH environment variable.

If py.exe is not on your Windows computers, then it will get installed when you install python (which is described below). If this is the case, you can skip down to the section below titled "Install python".



Now, to see what version of python is installed, you type:

Py -0p

As you can see in the screenshot below, this computer is running version 3.9-64. Remember, the OpenDxl python client runs on python 3.8 or 3.9. So, in this example Windows computer, it is ready to run the OpenDxl python client. If the version is not either 3.8 or 3.9, then we need to download and install python version 3.9. If this is the case in your environment, you can skip down to the section below titled "Install python".



Install python

Please go to <u>https://www.python.org/downloads/release/python-3910/</u> to download python 3.9.10. Scroll all the way to the bottom of the page to get the Windows downloads as shown in the screenshot below.

Files							
Version	Operating System	Description		MD5 Sum		File Size	GPG
Gzipped source tarball	Source release			1440acb71471	e2394befdb30b1a958d1	25800844	SIG
XZ compressed source tarball	Source release			e754c4b22767	50fd5b4785a1b443683a	19154136	SIG
macOS 64-bit Intel-only installer	macOS	for macOS 10.9 and later,	deprecated	2714cb9e6241	cf7e2f9022714a55d27a	30395760	SIG
macOS 64-bit universal2 installer	macOS	for macOS 10.9 and later		c2393ab11a42	3d817501b8566ab5da9f	38217233	SIG
Windows embeddable package (32-b	it) Windows			c1d2af96d9f35	64f57f35cfc3c1006eb	7671509	SIG
Windows embeddable package (64-b	it) Windows			b8e8bfba8e56	edcd654d15e3bdc2e29a	8509821	SIG
Windows help file	Windows			784020441c1a	25289483d3d8771a8215	9284044	SIG
Windows installer (32-bit)	Windows			457d648dc8a7	1b6bc32da30a7805c55b	27767040	SIG
Windows installer (64-bit)	Windows	Recommended		747ac35ae667	4ec1ee3b001e9b7dbc6	28909456	SIG
File Home Share	View ut opy path aste shortcut	Delete Rename	New folder	ew item 🔻 asy access 👻 v	Properties	Select	all none selection ect
← → ~ ↑ ↓ > This PC	> Downloads	-					
✓ Quick access	Name 🗠 Todav (1) ————	Date mo	dified	Туре	Size		
🖶 Downloads 🛛 🖈	b python-3.9.10-amd	64.exe 1/15/202	4 1:49 PM	Applicati	on 28,232 K	B	
Documents 🖈			double alie	k to incto	u.		
lesson en construire - Personal			double clic	ak to insta			
💻 This PC							





🄄 Python 3.9.10 (64-bit) Setup		_		×			
	Advanced Options						
	Associate files with Python (requires the py launcher)						
	Create shortcuts for installed applications						
Add Python to environment variables							
Precompile standard library							
Download debugging symbols							
	Download debug binaries (requires VS 2017 or later)						
1 / Constant							
	Customize install location						
	C:\Program Files\Python39		Brows	e			
python							
for							
windows	Back 💙 Instal		Cance	el l			



Now that you have installed python, you can go to the section titled "Checking for an existing python install" above if you want to ensure your python environment is correctly configured. You can also verify the installation in the Windows "Control Panel" as shown in the screenshot below.

Programs and Features				_	o x
← → × ↑ 🖬 > Control F	Panel > Programs > Programs and Features			✓ ♂ Search Programs	and F 🔎
Control Panel Home View installed updates	Uninstall or change a program To uninstall a program, select it from the lis	t and then click Uninstall, Change, or Repair.			
off	Organize 🔻			:=	: • 🕜
	Name Python 3.9.10 (64-bit) Python Launcher	Publisher Python Software Foundation Python Software Foundation	Installed On Size 1/15/2024 110 MB 1/15/2024 1.86 MB	Version 3.9.10150.0 3.9.7686.0	~
	Currently installed programs T 127 programs installed	otal size: 31.8 GB			

Install the OpenDxl python client

In the secRMM directory C:\Program Files\secRMM\AdminUtils\OpenDxl, there is a PowerShell script named GetOpenDxlClient.ps1 as shown in the screenshot below. The PowerShell script GetOpenDxlClient.ps1 will download and then install the OpenDxl python client.

		Name	Date modified	Туре	Size
Quick access		Cache	1/15/2024 1:25 PM	File folder	
secKMM	R	🗟 common.py	12/8/2023 3:01 PM	Python File	1 KB
Downloads	*	GetOpenDxIClient.ps1	1/14/2024 3:54 PM	Windows PowerS	4 KB
Documents	*	PythonPath.txt	1/15/2024 6:09 AM	Text Document	0 KB
OneDrive - Personal		secRMMOpenDxI.cmd	12/8/2023 3:54 PM	Windows Comma	2 KB
oneonice i cisonar		🙀 secRMMOpenDxI.ps1	1/15/2024 6:53 AM	Windows PowerS	27 KB
This PC		secRMMOpenDxI.ps1.log	1/11/2024 12:12 PM	LOG File	0 KB
🕽 3D Objects		📄 secRMMOpenDxI.py	1/15/2024 5:25 AM	Python File	9 KB
Desktop		secRMMOpenDxI.py.log	1/11/2024 12:12 PM	LOG File	0 KB
Documents		secRMMOpenDxIDisable.cmd	1/11/2024 12:43 PM	Windows Comma	1 KB
Downloads		secRMMOpenDxIEnable.cmd	1/11/2024 12:43 PM	Windows Comma	1 KB

To run the PowerShell script GetOpenDxlClient.ps1, open a Windows command window (as Administrator) and "change directory" (CD) into the directory C:\Program Files\secRMM\AdminUtils\OpenDxl as shown in the screenshots below.

Command Prompt App Apps x64 Native Tools Command Prompt for VS 2017	>	Command Prompt App
 Node, Js command prompt x86_x64 Cross Tools Command Prompt for VS 2019 Settings Replace Command Prompt with Windows PowerShell in the Win + X Search the web 	> >	□ Open □ Run as administrator □ Open file location □□ Open file location □□ Pin to Start □□ Pin to taskbar
 cmd - See more search results cmd administrator cmd ipconfig cmd commands cmd prompt 	> > > >	

B Administrator: Command Prompt	_	×
Microsoft Windows [Version 10.0.19045.3930] (c) Microsoft Corporation. All rights reserved.		^
C:\Windows\system32>cd "\Program Files\secRMM\AdminUtils\OpenDx1" now hit enter		
Case Administrator: Command Prompt	_	×
Microsoft Windows [Version 10.0.19045.3930]		^

(c) Microsoft Corporation. All rights reserved. C:\Windows\system32>cd "\Program Files\secRMM\AdminUtils\OpenDxl" C:\Program Files\secRMM\AdminUtils\OpenDxl>



If there were no errors returned, you have successfully installed the OpenDxl python client onto the Windows computer. If by chance you did receive errors, please check if they are related to accessing the internet. This will usually be a firewall issue and/or a proxy server issue. If you need help, please email support@squadratechnologies.com and we would be happy to provide our free technical assistance over a screensharing session or a phone call if you cannot share your screen.

Configure secRMM to send security events to the OpenDxl fabric/servers

The secRMM property that tells secRMM to send the secRMM security events to the OpenDxl fabric/servers is named SendToOpenDxl as shown in the screenshots below.

All Apps Documents Web More	÷	×
 Best match		
Computer Management		
Settings		Computer Management
🗾 View advanced system settings	>	Арр
Search the web		
Computer management - See more search results	>	☐ Open
computer management windows 10	>	
computer management local users groups	>	- Pin to Start
𝒫 computer management user	>	∽ Pin to taskbar
computer management windows 11	>	
, computer management console	>	
, computer management software	>	
, computer management system	>	
𝒫 computer management cmd	>	
𝒫 computer management app	>	
♀ computer management		



secRMM OpenDxl Administrator Guide

🜆 Computer Management			– 🗆 X
File Action View Help			
🗢 🏟 🔰 📰 🔢 🖬			
🜆 Computer Management (Local)	Computer Configuration		Actions
 Computer Management (Local) System Tools Task Scheduler Event Viewer Event Viewer Shared Folders Solution Company Performance Device Manager Storage Toisk Management Services and Applications 	Computer Configuration Name AllowedDirectories AllowedDirectories AllowedFileExtensions AllowedPrograms AllowedSerialNumbers AllowedSerialNumbers AllowedSerialNumbers AllowedSerialNumbers AllowedUsers BlockCDROMAndDVDWrites BlockOfficeMacrosOnDevice EnableRMS FailWriteHSourceFileUnknown HashAlgorithm InstallDateTime LogSecurityEventsAsFailures LogWriteDetails MonitorCDROMAndDVD MonitorCDROMAndDVD MonitorCDROMAndDVD MonitorCDROMAndDVD MonitorEloppyDrive PreApproveSafeCopy RequireFingerPrin	Value Value 01/15/2024 13:25:39 on click this row.	Actions secRMM Image: SafeCopy Approver Image: Device Tracker Image: SecRMM License Image: SecRMM Configurations View Image: SecRMM Configurations View Image: SecRMM Configurations View Image: SecRMM Configurations View Image: SecRMToOpenDxl Edit Image: Refresh Image: Help
	Send to reams		
	Syslog Version	9.11.26.0	

Computer Management (Local)	Computer Configuration		Actions
👔 System Tools	Name	Value	Ph4h4
> 🕒 Task Scheduler	AllowBitLockerOphy		SECTIVITY
> 🛃 Event Viewer	AllowedDirectories		8 SafeCopy Approver
> 🧉 secRMM	AllowedFileExtensions		🛔 Device Tracker
> 👸 Shared Folders	AllowedInternalIds		
> 🜆 Local Users and Groups	AllowedPrograms		seckiviivi License
> 🔊 Performance	Allowed Serial Numbers		📒 📒 secRMM Configurations
Device Manager	AllowedUsers		View
Storage	BlockCDROMAndDVDWrites		
E Disk Management	BlockOfficeMacrosOnDevice		I Help
Services and Applications	Block ProgramsOn Devid		
	EnableRMS SecRM	/IM OpenDxI	- 0 ×
	FailWritelfSourceFileUn		
	HashAlgorithm Mode: Co	omputer , Computer Config: W9	
	InstallDateTime Dxl Com	fig File:	
	LogSecurityEventsAsFa		
	LogWriteDetails Format:	~	
	MonitorCDROMAndDV		
	MonitorFloppyDrive ONL	INE	^
	PreApproveSafeCopy OFF	LINE	
	RequireAzureVC WR	TE SUCCESS	
	RequireFingerPrint WRI	TEFAILURE	
	RequireMDMEnrollment ADM	INISTRATION	×
	RequireSmartCard		
	RequireSmartPhoneLog	Apply Clear	Send test
	ScanDevice	OK Caree	
	SCCMConnection	OK Cance	1
	SendEmail		
	SendToAzureLog		
	SendToOpenDxl		
	SendToTeams		
	SNMP		
	Syslog		

As you can see in the screenshot above, we need to supply 3 values to connect secRMM to the OpenDxl fabric/servers:

- 1. An OpenDxl Configuration File (detailed below in the section titled "OpenDxl Configuration File")
- 2. The data format you want secRMM to use when sending the security events to the OpenDxl fabric/servers. As you can see in the screenshot below, the data format legal values are:
 - a. csv
 - b. xml
 - c. html
 - d. json

SecRMM OpenDxI -		×
Mode: Computer , Computer Config: W9		
Format:		
ONLINE xml OFFLINE html UPFLINE ison	^	
	¥	
Apply Clear Send test		
OK Cancel		

- 3. Which secRMM removable storage security event to send to the OpenDxl fabric/servers. As you can see in the screenshot below, the removable storage security event legal values are:
 - a. ONLINE
 - b. OFFLINE
 - c. WRITE SUCCESS
 - d. WRITE FAILURE
 - e. ADMINISTRATION
 - f. LICENSING
 - g. EXTERNAL

ONLINE	
OFFLINE	
WRITE SUCCESS	
WRITE FAILURE	
ADMINISTRATION	
LICENSING	
EXTERNAL	

OpenDxl Configuration File

Generating the OpenDxl configuration file is a function that is dependent on the OpenDxl fabric/server software so the screenshots in this section will likely not be the steps you will perform in your environment. If you are not the system administrator for your OpenDxl fabric/server, you will need to work with the system administrator for the OpenDxl fabric/server in your environment. If you need help, please email support@squadratechnologies.com and we would be happy to provide our free technical assistance over a screensharing session or a phone call if you cannot share your screen.

Go to the 'Certificate Management' section in your OpenDxl Fabric/server as shown in the screenshots below.

📴 OpenDXL Brol	ker Console × +				
d ⊳ e	<u>۵</u> ۵	Not secure https://localhost:8443			
	Fabric Monitor				
₽	Services *				
		Type: Event			
÷	Click once	Topic :			
Eg ∕		Payload :			
	Certificate Management				
	No services found on fabric.				
		Send Message			
		Received Messages			
		Filter by Type: 🔶 Events ⊃ Responses 🕕 Errors			
		Туре Торіс	Payload		
		•			
	Subscriptions				
	Add		No messages have been received.		
OpenDXL Broker Console	No subscriptions have been added.				

Fill out this form and then click the generate button.

OpenDXL Bro	ker Console × +		
4 D C		Not secure <u>https://localhost:</u>	3443
	Generate Configuration		
M.	Configuration Type :	Client Configuration 🗸]
	Common Name :		(e.g. server FQDN or YOUR name)
모	Country Name :		(2 letter code)
	State or Province Name :		(full name)
	Locality Name :		(eg, city)
=0	Organization Name :		(eg, company)
	Organizational Unit Name :		(eg, section)
	Email Address :		
	Generate		
OpenDXL Broker Console			
Version: 0.3.3			
(?)			
Logout			

The Generate function will create 4 files as shown in the screenshot below. The dxclient.config file points to the other 3 files (which contain the security credentials required to connect to the OpenDxl fabric/servers).

File Home	Share V	/iew																				
Pin to Quick Copy access	Paste	t py path ste shortcut	Move Copy to •	Delete Rename	New folde	r New item ▼ T Easy access ▼	Properties	pen ▼ 📑														
Clij	oboard		Organize New			Open																
← → ~ ↑ 🔄 > This PC > D drive (D:) > Projects > Squadra > secRMM > OpenDxI > OpenDxIConfig																						
🕹 Quick access		Name		Date modified		Туре	Size															
		🔄 ca-broke	er.crt	12/9/2023 3:53 PM		Security Certificate	3 KB															
SECRIVIIVI	ads 🖈	<i>ж</i>		7	7	7	7	7	7		7	7	ж		<i>ж</i>	🔄 client.cr	t	12/9/2023 3:53 PM		Security Certificate	2 KB	
Downloads		 ✓ Client.key ✓ dxlclient.config 		12/9/2023 3:53 PM 12/10/2023 11:43 AM		KEY File	2 KB															
🚆 Documents	*					XML Configuratio	1 KB															
📥 OneDrive - Per	sonal																					
💻 This PC																						

As described in the section above, you will specify the dxlclient.config path when setting the secRMM SendToOpenDxl property.

SecRMM OpenDxI -	ı x
Mode: Computer , Computer Config: W9	
Dxl Config File:	
Format:	
ONLINE OFFLINE WRITE SUCCESS WRITE FAILURE ADMINISTRATION	• •
Apply Clear Send test	
UK Cancer	
SecRMM OpenDxI - C X Search OpenDx	xlConfic
Mode: Computer , Computer Config: W9	
Format: 1. cate 3 K	KB
ONLINE OpenDxl Config File	×
□ WRITE SUCC □ WRITE FAILU ← → ~ ↑ □ « Projects → Squadra → secRMM → OpenDxl → OpenDx	xIConfig v 👌 Search OpenDxIConfig 🔎
ADMINISTRA Organize Vew folder	E 🕶 🔳 😮
Ap secRMM 🖈 ^ Name ^	Date modified Type Size
🕂 Downloads 🛷 🔄 ca-broker.crt	12/9/2023 3:53 PM Security Certificate 3 KB
🔮 Documents 💉 🙀 client.crt	12/9/2023 3:53 PM Security Certificate 2 KB
OneDrive - Personal	12/9/2023 3:53 PM KEY File 2 KB
dxlclient.config 2.	12/10/2023 11:43 AM CONFIG File 1 KB
This PC 🗸	
9 1 File name: dylclient.confin	3. ~
	Open Cancel

You might consider storing these 4 files on a network share and then specifying the network share when pointing secRMM to the dxlclient.config file. This has the advantage of having the files in one spot and not replicated. However, the disadvantage is that the network share would need to be online when the endpoint computers needed to read the files.

Data format and which secRMM events

Specify the data format and the secRMM removable storage security events and then click the OK button to save the secRMM SendToOpenDxl property as shown in the screenshot below.

SecRMM	OpenDxI				_		×
Mode: Comp	uter , Compu	ter Config: WS	Ð				
Dxl Config F	ile: D:\Proje	ects\Squadra\	secRM	M\OpenD	d\OpenD>	dCo	
Format:	html		~	1.			
V RITES V RITES ADMINIS LCENSI	SUCCESS FAILURE STRATION NG	2.				^	
	IAL					~	
	Apply	Clear OK	Cano	Send te	st		

secRMM OpenDxl Administrator Guide

🜆 Computer Management			- 🗆 X
File Action View Help			
🛃 Computer Management (Local)	Computer Configuration		Actions
🗸 🎁 System Tools	Name	Value	secRMM 🔺
> 🕒 Task Scheduler	AllowBitLockerOnly		
> 🛃 Event Viewer	AllowedDirectories		85 SafeCopy Approver
> 🧉 secRMM	AllowedFileExtensions		A Device Tracker
> 👸 Shared Folders	AllowedInternalIds		= cecRMM License
> 🜆 Local Users and Groups	AllowedPrograms		secrivity License
> 🔕 Performance	AllowedSerialNumbers		secRMM Configurations
🚦 Device Manager	AllowedUsers		View 🕨
✓ Image Storage	BlockCDROMAndDVDWrites		
Disk Management	BlockOfficeMacrosOnDevice		Help
Services and Applications	Block ProgramsOn Device		SandToOpenDyl A
1 100	EnableRMS		Send to OpenDX1 _
	FailWritelfSourceFileUnknown		Edit
	HashAlgorithm		Refresh
	InstallDateTime	01/15/2024 13:25:39	
	LogSecurityEventsAsFailures		[Help
	LogWriteDetails		
	MonitorCDROMAndDVD	on	
	MonitorFloppyDrive		
	PreApproveSafeCopy		
	RequireAzureVC		
	RequireFingerPrint		
	RequireMDMEnrollment		
	RequireSmartCard		
	RequireSmartPhoneLogin		
	ScanDevice		
	SCCMConnection		
	SendEmail		
	SendToAzureLog		
	SendToOpenDxl	D:\Projects\Squadra\secRMM\OpenDxl\OpenDxlConfig\dxlclient.config	
	SendToTeams		
	SNMP		
	Syslog		
	Version	9.11.26.0	

Configure the OpenDxl fabric/servers to receive secRMM events

Generating the OpenDxl subscription to receive the secRMM removable storage security events is a function that is dependent on the OpenDxl fabric/server software so the screenshots in this section will likely not be the steps you will perform in your environment. If you are not the system administrator for your OpenDxl fabric/server, you will need to work with the system administrator for the OpenDxl fabric/server in your environment. If you need help, please email support@squadratechnologies.com and we would be happy to provide our free technical assistance over a screensharing session or a phone call if you cannot share your screen.

Click the "Add" button under the Subscriptions label as shown in the screenshot below.

OpenDXL Bro	oker Console × +			~ - 0 X
d D C	Not secure https://	/localhost:8443	2 🛛 🗘 🗖 🖬	🖢 💿 VPN 🛛 Update 🚍
	Fabric Monitor			
A C	Services *	Send Message		
÷		Type : Event Topic :		
Ē₽	No services found on fabric.	Payload :		
		Send Message		
	Subscriptions click once			
	🔾 Add	Received Messages		
OpenDXL Broker Console		Filter by Type: 🛏 Events ⊃ Responses Errors		
Version: 0.3.3		Type Topic Pa	ayload	Date
Image: Content of the second s	No subscriptions have been added.	No messages h	nave been received.	

In the entry field, type:

/secRMM

Don't forget the forward slash (/) as the first character.

Make sure that sec is lower case.

Make sure that RMM is upper case.

Now click off the entry field so the user interface accepts the text (/secRMM).

The OpenDxl fabric/server is now listening for the secRMM removable storage security events

OpenDXL Bro	ker Console X	+								Ý		
⊲ ⊳ e				/localhost:844	13			2	۵ 🕲	7	O VPN	Update \equiv
	Fabric Monitor											
₽d	Services		•	Send M	essage							
÷				Type : Topic :	Event		•]			
Ē₽	No servic	ces found on fabri	c.	Payload :								
			****	Send	Message							
	Subscriptions			A Receive	ed Messages							
OpenDXL Broker Console	Add /secRMM		•	Filter by Typ	e: 🔶 Events	Responses	Errors					
Version: 0.3.3				Туре	Торіс			Payload				Date
(?) Logout							No messag	ges have been	received.			

Send a test security event from secRMM to the OpenDxl fabric/servers

Once you have completed the above configuration steps, you can test the secRMM connection to the OpenDxl fabric/servers using the Windows Computer Management tool.

🜆 Computer Management			- 🗆 X
File Action View Help			
🔶 🄿 🙍 📰			
Local)	Computer Configuration		Actions
 Computer Management (Local) System Tools Task Scheduler Task Scheduler SecRMM SecRMM Solar Schard Folders Local Users and Groups Cource Manager Storage Disk Management Services and Applications 	Computer Configuration Name AllowedDirectories AllowedFileExtensions AllowedSeralNumbers AllowedSeralNumbers BlockCDROMAndDVDWrites BlockCRPogramsOnDevice BlockCPROMAndDVD HashAlgorithm InstallDateTime LogSecutyEventsAsFailure LogWriteDetails MontorCDROMAndDVD MontorCDROMANdDVD MontorCDROMANDDVD PreApproveSafeCopy RequireMDMErrollment RequireMDMErrollment RequireMDMErrollment RequireMDMErrollment SendToAzureLog SendToAzureLog SendToAzureLog SendToTeams SNMP Syslog Version	Value RMM OpenDxl Computer . Computer Corfig: W9 onfig File: assecRMM:OpenDxlOpenDxlConfig'ddxClient.config multime FFLINE RITE FAILURE MINISTRATION OK Cancel D:\Projects\Squadra\sec RMM\OpenDxl\OpenDxl\OpenDxl\OpenDxlConfig\ddxClient.config 9.11.26.0	Actions secRMM SecRMM Device Tracker SecRMM License SecRMM Configurations View Help SendToOpenDxl Edit Refresh Help Help



OpenDXL Bro	ker Console × +		V	- 0 X			
⊲ ⊳ e	A Not secure http://www.accord.com/accord/acco	ss ://localhost:8443	2 V 🖉 🛆 🛛 🖬	● VPN Update ☰			
Fabric Monitor							
	Services *	❀ Send Message					
	No services found on fabric.	Type : Event Topic : Payload :					
		Send Message					
	Subscriptions	Received Messages					
OpenDXL	Add						
Broker Console	/secRMM	Filter by Type: 🛏 Events ⊃ Responses 🔮 Errors					
Version: 0.3.3	Туре Торіс	Pavload	Date				
0		👄 Event /secRMM	<th colspan="2" bgcolor="Yello</th> <th>Jan 15, 2024 15:22:47</th>	Jan 15, 2024 15:22:47			
		👄 Event /secRMM	secRMM test message: User Tony on computer W9:	Jan 15, 2024 15:22:47			
Logout							

If you double click the event, it will open a new window with the event details as shown in the screenshot below. When you run the secRMM test function, you will receive 2 events, the first one is saving the secRMM SendToOpenDxl property. secRMM generates security events for any secRMM policy changes...not only does it monitor your end-users, it also monitors the administrators too!

Message De	tails	<
ID:	{9adafb08-2071-4ad7-ae52-925e598a2f95}	٦
Topic:	/secRMM	1
Type:	Event	
Payload:	cp> secRMM test message: User Tony on computer W9: DxlClientConfigFile = D:\Projects\Squadra\secRMM\OpenDxl\OpenDxlConfig\dxlclient.config, DxlDataFormat = htm	1
Source Broker:	4a61959a-f742-4681-bb1e-2b218917cd45	
Source Client:	99bc360cf0cd5e901fd217fd809d320dac47c12a	
Other Fields:	{ "dxl.certs": "faf6510a01c0871e93031e8f478933303879e803;99bc360cf0cd5e901fd217fd809d320dac47c12a" }	
Date:	1/15/2024, 3:22:47 PM	1
<		>

Contacting Squadra Technologies Support

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

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

4. The specific issue you are contacting support for.

About Squadra Technologies, LLC.

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

Contacting Squadra Technologies, LLC.

Phone	562.221.3079
Email	info@squadratechnologies.com
Mail	Squadra Technologies, LLC.
	World Headquarters
	4201 State Route W
	Cleveland, Missouri 64734
	USA
Web site	http://www.squadratechnologies.com/