



Security Removable Media Manager

OpenDxl Administrator Guide

Version 9.11.26.0

(January 2024)

Protect your valuable data



secRMM OpenDxl Administrator Guide

© 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 SECMMM 4

 PREREQUISITES FOR OPENDXL 5

Checking for an existing python install..... 5

Install python..... 6

Install the OpenDxl python client..... 10

 CONFIGURE SECMMM 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 SECMMM EVENTS..... 22

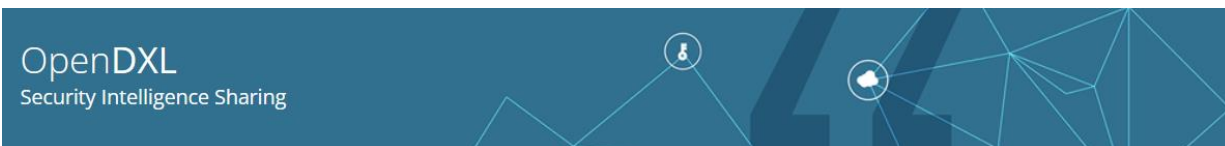
 SEND A TEST SECURITY EVENT FROM SECMMM TO THE OPENDXL FABRIC/SERVERS 24

CONTACTING SQUADRA TECHNOLOGIES SUPPORT 25

ABOUT SQUADRA TECHNOLOGIES, LLC..... 26

secRMM OpenDxl Administrator Guide

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 auditing 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:

<https://www.opendxl.com/>. 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: <https://opencybersecurityalliance.org/>. One such product on the market today is McAfee/Trellix enterprise Policy Orchestrator (ePO for short). You can read more about ePO at: <https://www.trellix.com/products/epo/>.

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.

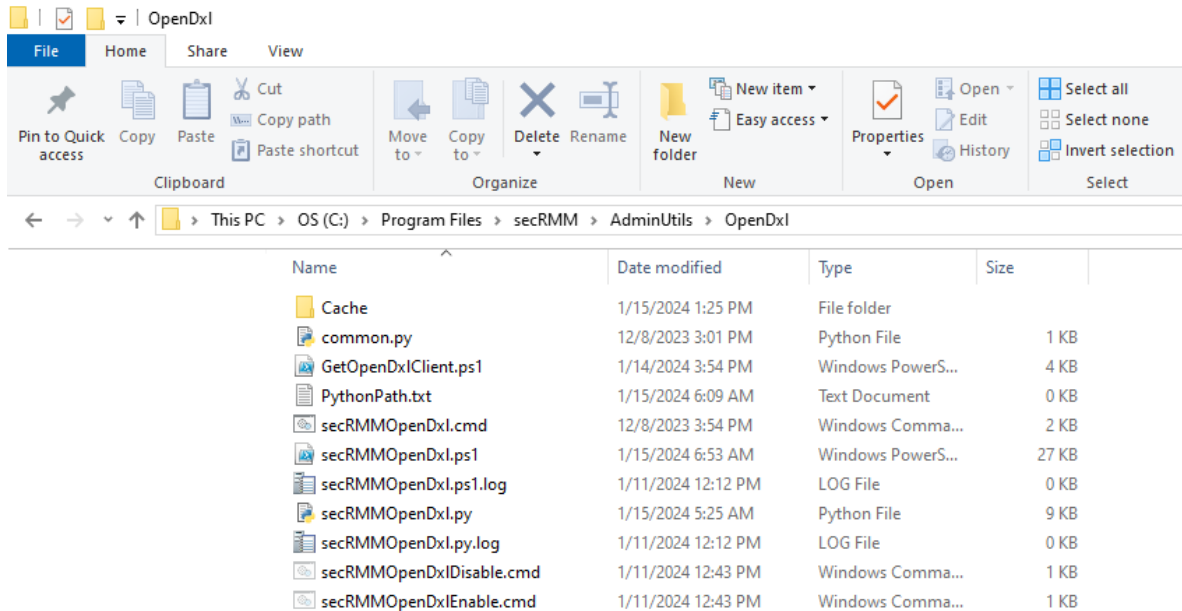
Installation of secRMM

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.squadrates.com/Products/secRMM/secRMMDocumentation.aspx> to get the tool that is used in your environment. If you need help getting started, please email support@squadrates.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.

secRMM OpenDxl Administrator Guide

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.



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.

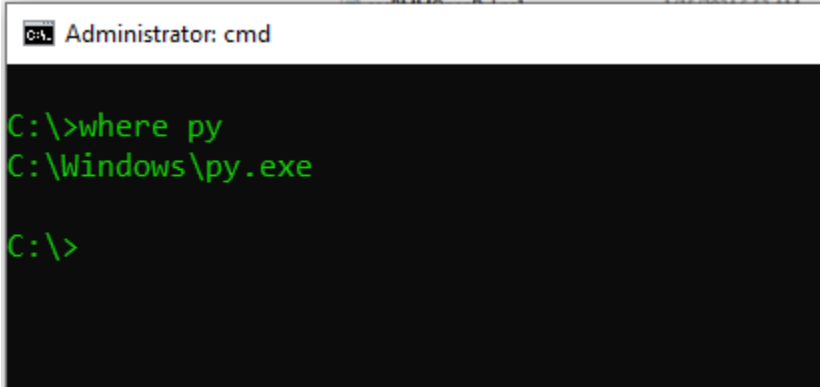
Open a command prompt window (running as administrator) and type:

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.

secRMM OpenDxl Administrator Guide

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”.

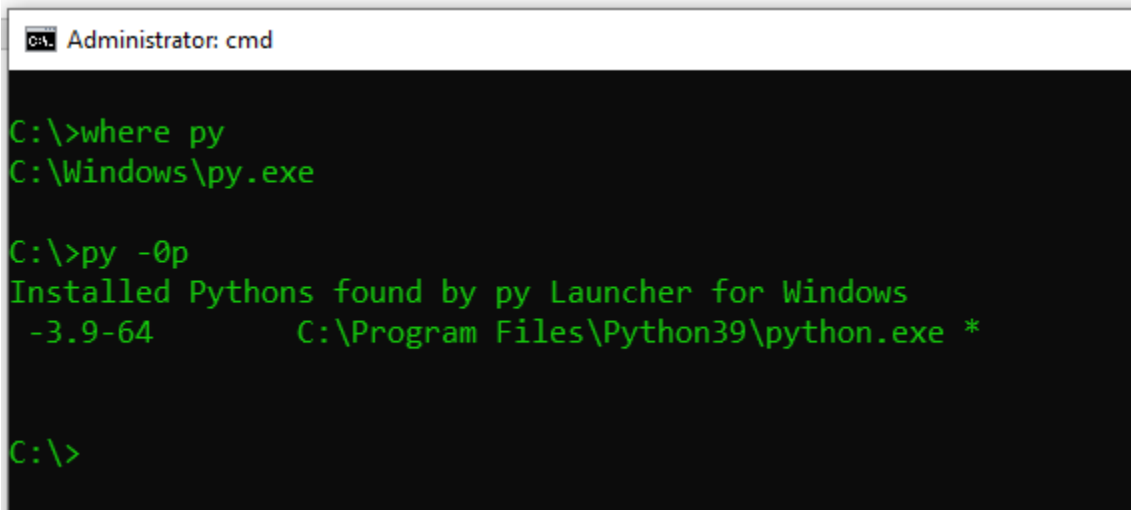


```
Administrator: cmd
C:\>where py
C:\Windows\py.exe
C:\>
```

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”.



```
Administrator: cmd
C:\>where py
C:\Windows\py.exe
C:\>py -0p
Installed Python's found by py Launcher for Windows
-3.9-64          C:\Program Files\Python39\python.exe *
C:\>
```

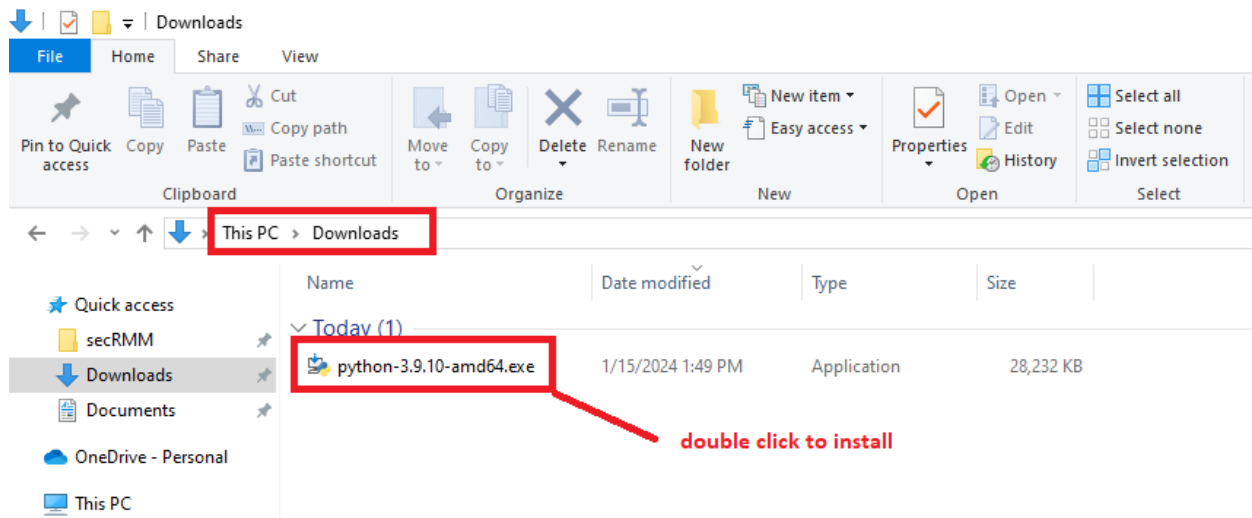
Install python

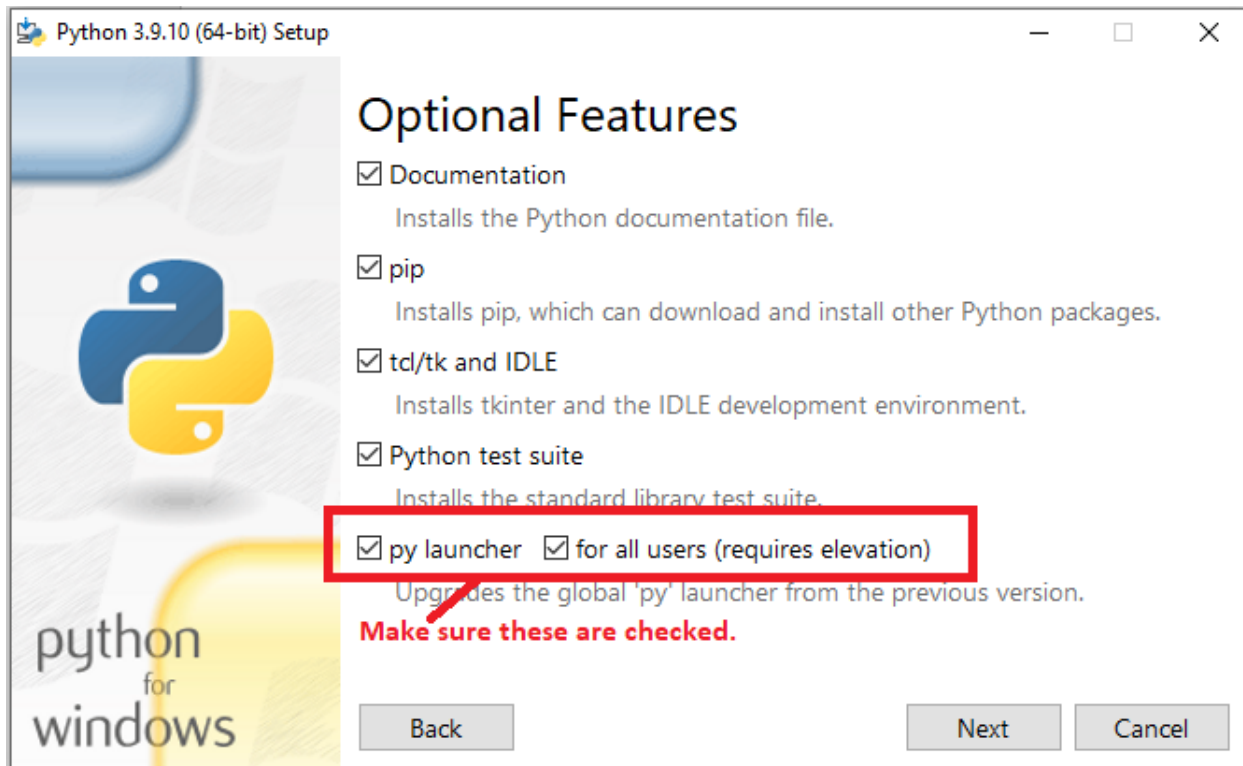
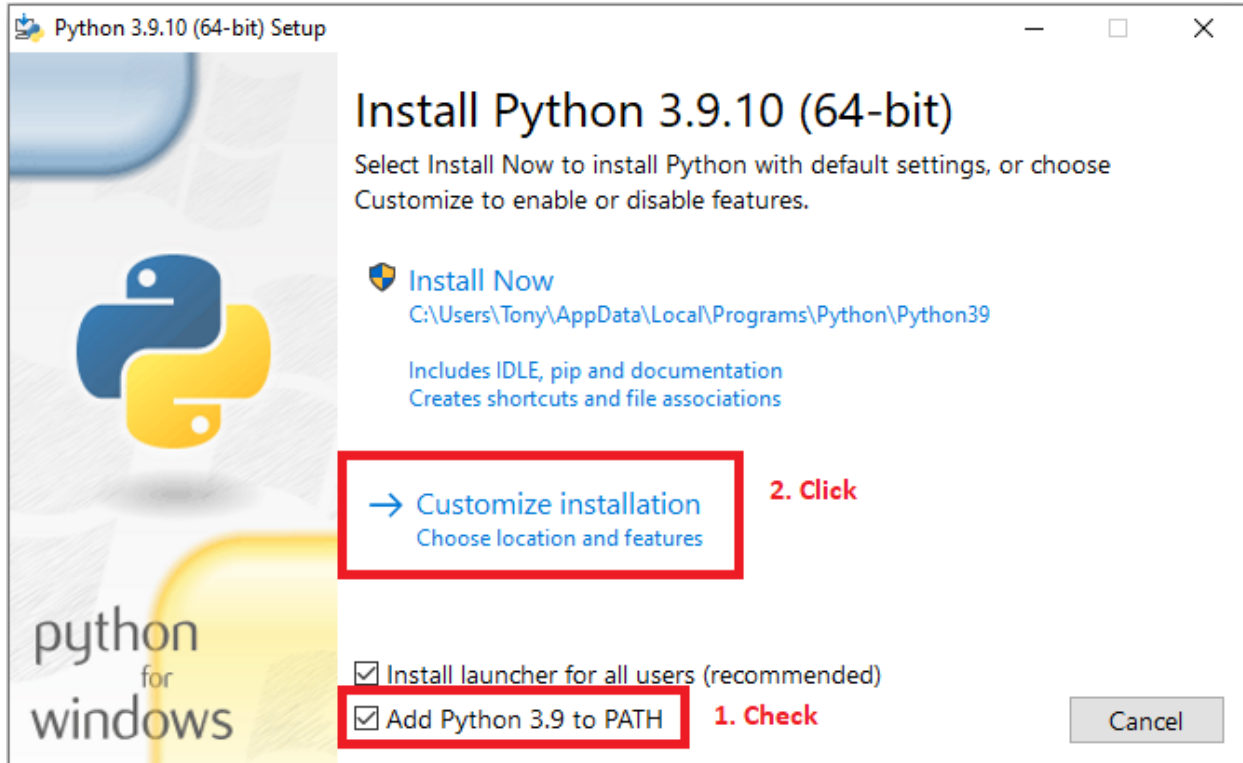
Please go to <https://www.python.org/downloads/release/python-3910/> to download python 3.9.10. Scroll all the way to the bottom of the page to get the Windows downloads as shown in the screenshot below.

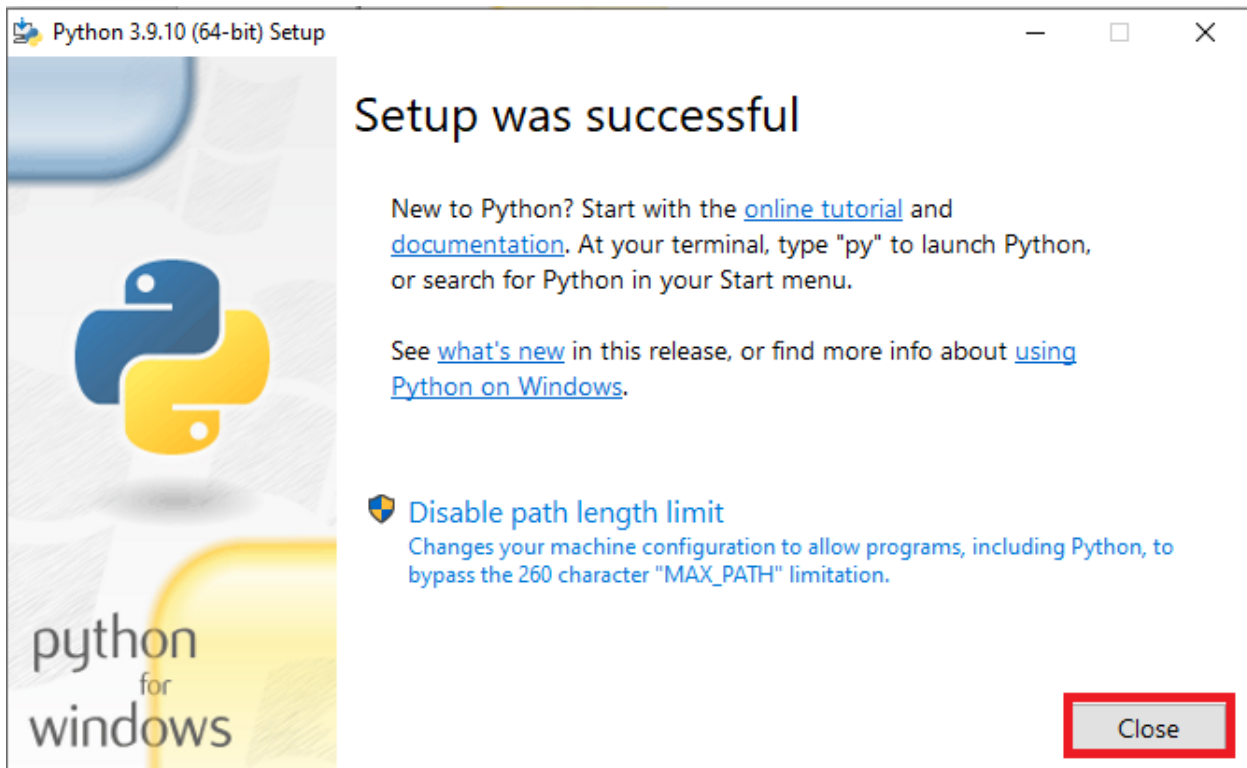
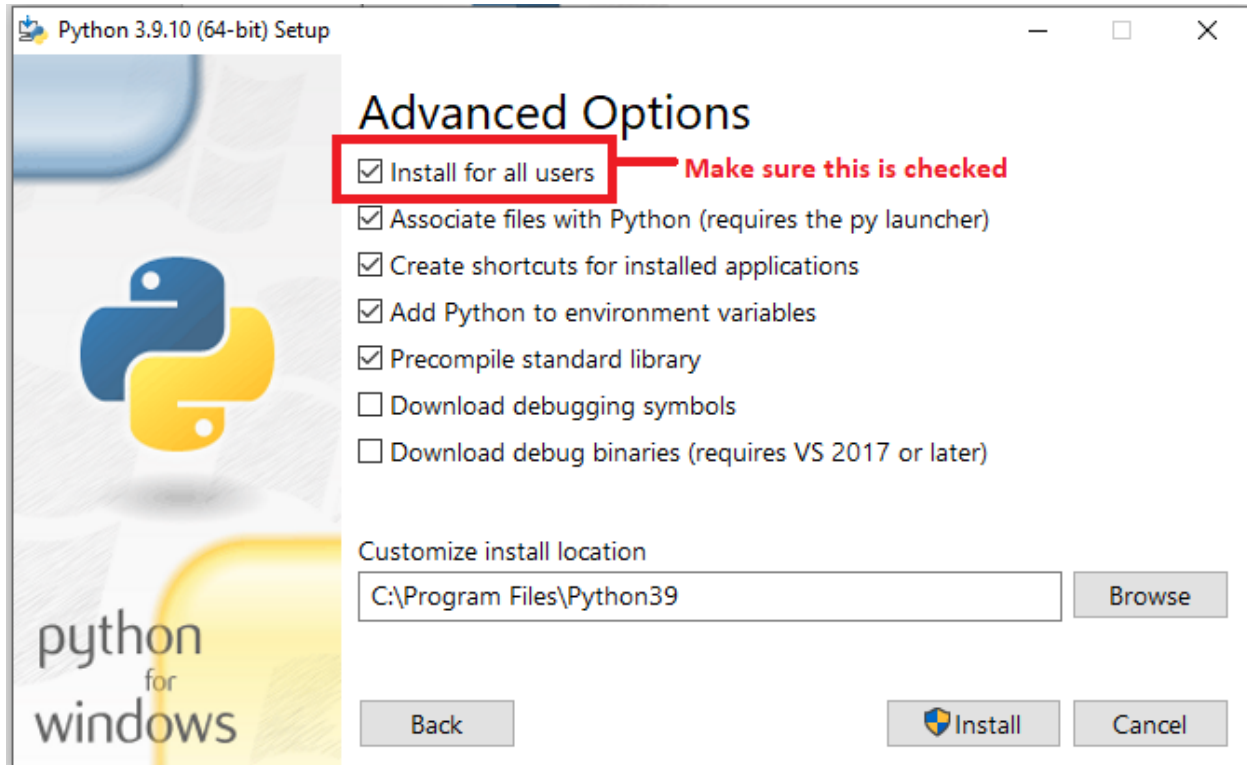
secRMM OpenDxl Administrator Guide

Files

| Version | Operating System | Description | MD5 Sum | File Size | PGP |
|---|------------------|--------------------------------------|----------------------------------|-----------|---------------------|
| Gziped source tarball | Source release | | 1440acb71471e2394befdb30b1a958d1 | 25800844 | SIG |
| XZ compressed source tarball | Source release | | e754c4b2276750fd5b4785a1b443683a | 19154136 | SIG |
| macOS 64-bit Intel-only installer | macOS | for macOS 10.9 and later, deprecated | 2714cb9e6241cf7e2f9022714a55d27a | 30395760 | SIG |
| macOS 64-bit universal2 installer | macOS | for macOS 10.9 and later | c2393ab11a423d817501b8566ab5da9f | 38217233 | SIG |
| Windows embeddable package (32-bit) | Windows | | c1d2af96d9f3564f57f35cfc3c1006eb | 7671509 | SIG |
| Windows embeddable package (64-bit) | Windows | | b8e8bfa8e56edcd654d15e3bdc2e29a | 8509821 | SIG |
| Windows help file | Windows | | 784020441c1a25289483d3d8771a8215 | 9284044 | SIG |
| Windows installer (32-bit) | Windows | | 457d648dc8a71b6bc32da30a7805c55b | 27767040 | SIG |
| Windows installer (64-bit) | Windows | Recommended | 747ac35ae667f4ec1ee3b001e9b7dbc6 | 28909456 | SIG |

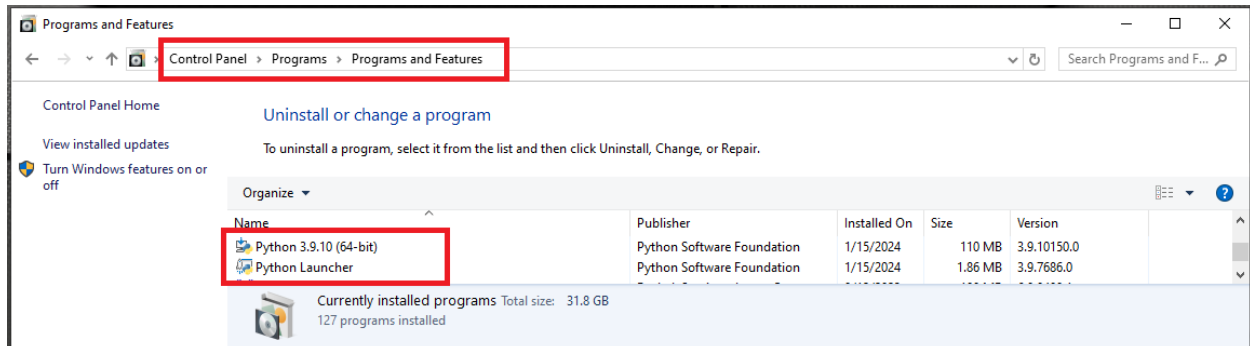






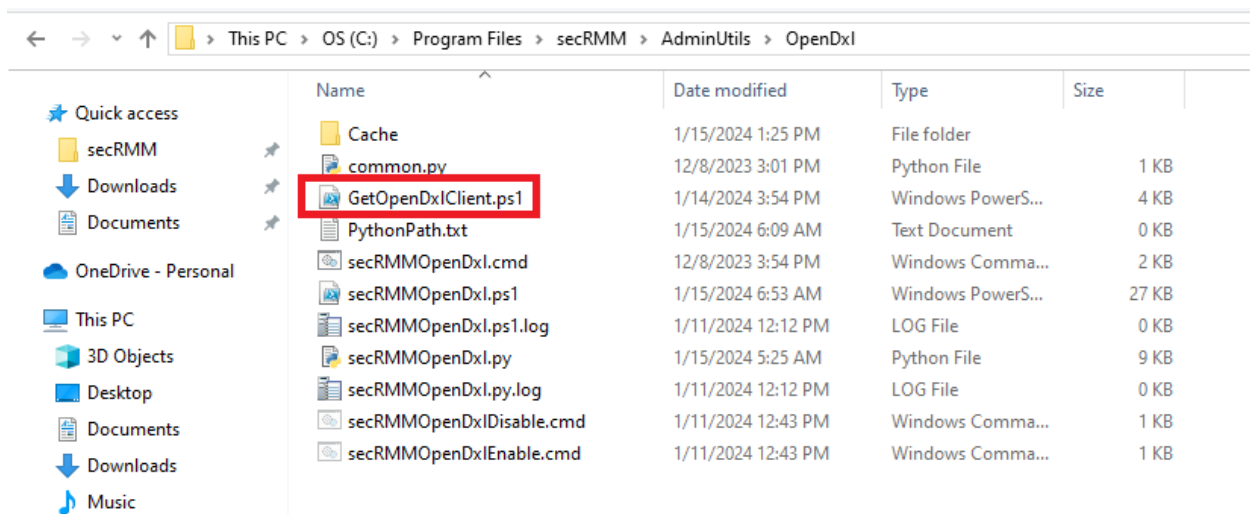
secRMM OpenDxl Administrator Guide

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.



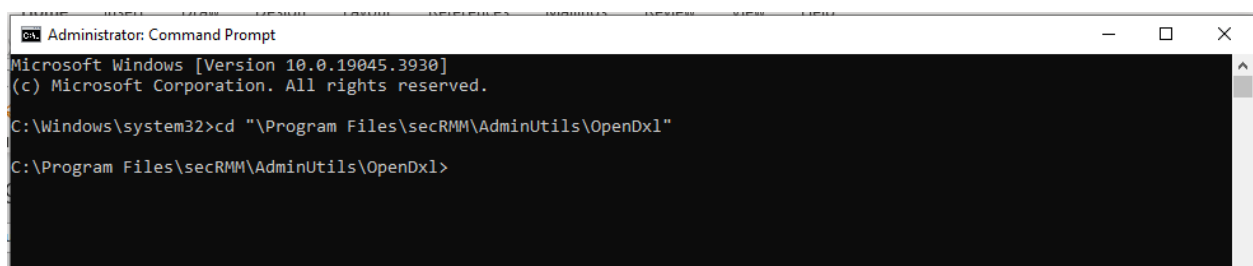
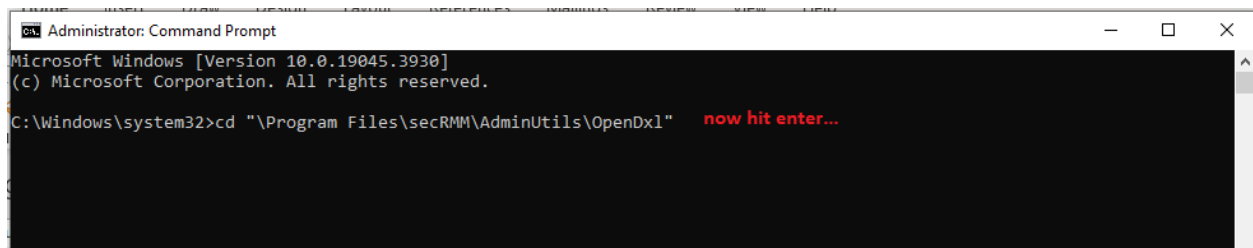
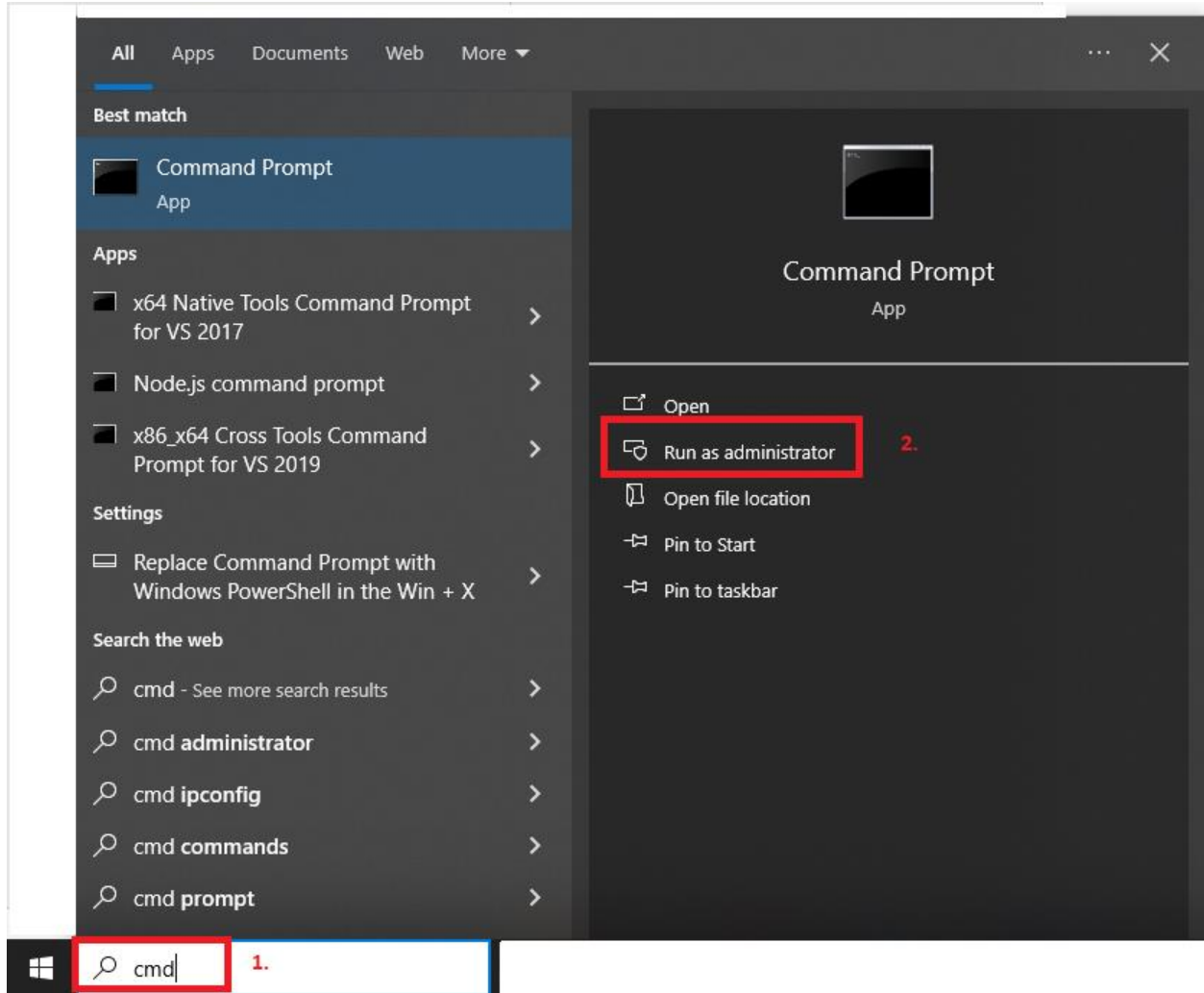
Install the OpenDxl python client

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.



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.

secRMM OpenDxl Administrator Guide



secRMM OpenDxl Administrator Guide

```
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>powershell .\GetOpenDxlClient.ps1  now hit enter...
```

```
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>powershell .\GetOpenDxlClient.ps1
pip 23.3.1 from c:\program files\python39\lib\site-packages\pip (python 3.9)
GetOpenDxlClient.ps1: download of https://files.pythonhosted.org/packages/30/2c/46757550aea6eea2b98f475fbb7c5a53eba7b36da5c5d40ad39af99b5ac5/dxclient-5.6.0.4-py2.py3-none-any.whl to file dxclient-5.6.0.4-py2.py3-none-any.whl succeeded.
GetOpenDxlClient.ps1: installing dxclient-5.6.0.4-py2.py3-none-any.whl.
Processing c:\program files\secrmm\adminutils\opendxl\dxclient-5.6.0.4-py2.py3-none-any.whl
Requirement already satisfied: asn1crypto in c:\program files\python39\lib\site-packages (from dxclient==5.6.0.4) (1.5.1)
Requirement already satisfied: configobj in c:\program files\python39\lib\site-packages (from dxclient==5.6.0.4) (5.0.8)
Requirement already satisfied: msgpack<1.0.0,>=0.5 in c:\program files\python39\lib\site-packages (from dxclient==5.6.0.4) (0.6.2)
Requirement already satisfied: oscrypto in c:\program files\python39\lib\site-packages (from dxclient==5.6.0.4) (1.3.0)
Requirement already satisfied: requests in c:\program files\python39\lib\site-packages (from dxclient==5.6.0.4) (2.31.0)
Requirement already satisfied: PySocks<1.7 in c:\program files\python39\lib\site-packages (from dxclient==5.6.0.4) (1.6.8)
Requirement already satisfied: six in c:\program files\python39\lib\site-packages (from configobj->dxclient==5.6.0.4) (1.16.0)
Requirement already satisfied: charset-normalizer<4,>=2 in c:\program files\python39\lib\site-packages (from requests->dxclient==5.6.0.4) (3.3.2)
Requirement already satisfied: idna<4,>=2.5 in c:\program files\python39\lib\site-packages (from requests->dxclient==5.6.0.4) (3.6)
Requirement already satisfied: urllib3<3,>=1.21.1 in c:\program files\python39\lib\site-packages (from requests->dxclient==5.6.0.4) (2.1.0)
Requirement already satisfied: certifi>=2017.4.17 in c:\program files\python39\lib\site-packages (from requests->dxclient==5.6.0.4) (2023.11.17)
dxclient is already installed with the same version as the provided wheel. Use --force-reinstall to force an installation of the wheel.

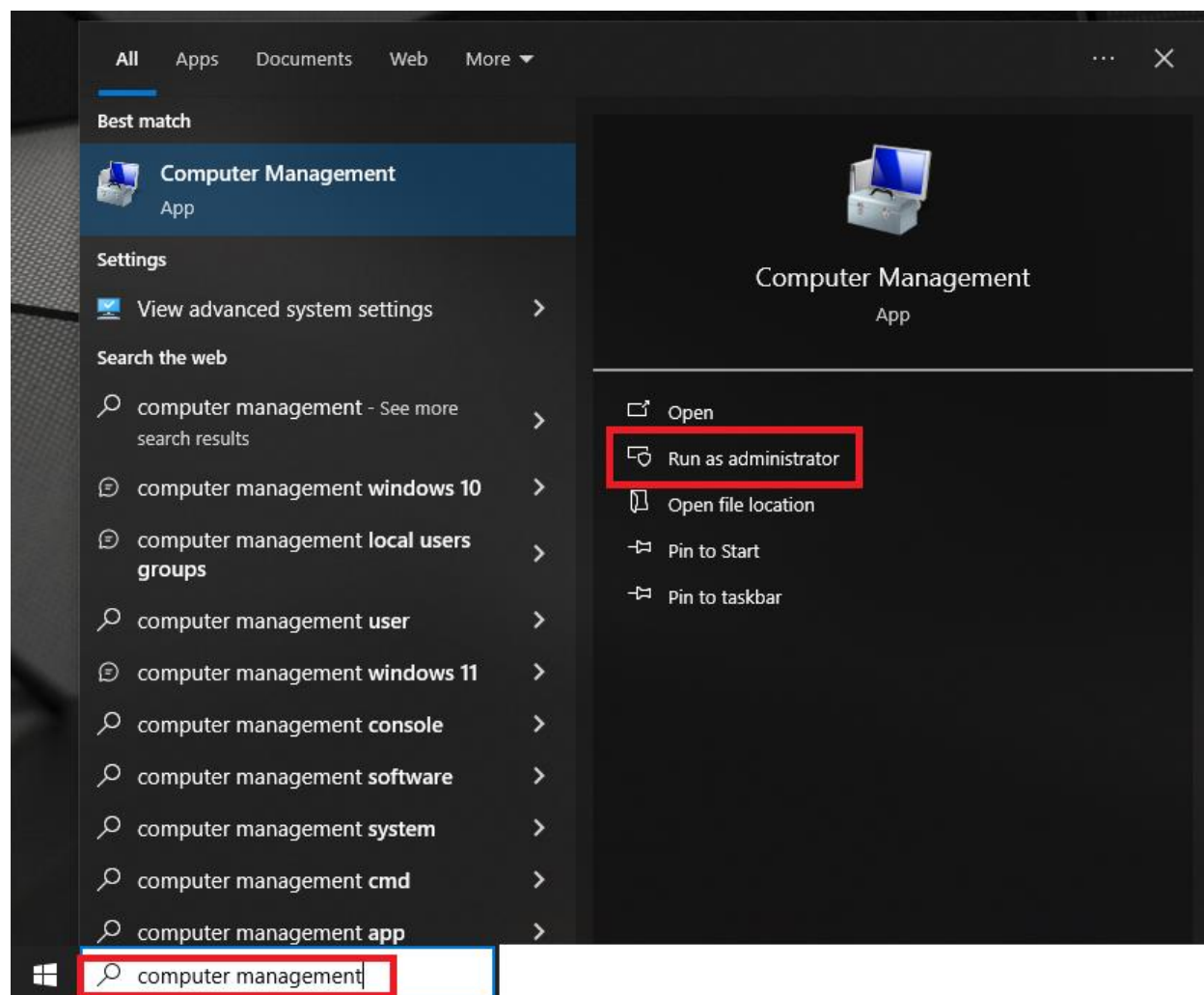
[notice] A new release of pip is available: 23.3.1 -> 23.3.2
[notice] To update, run: python.exe -m pip install --upgrade pip

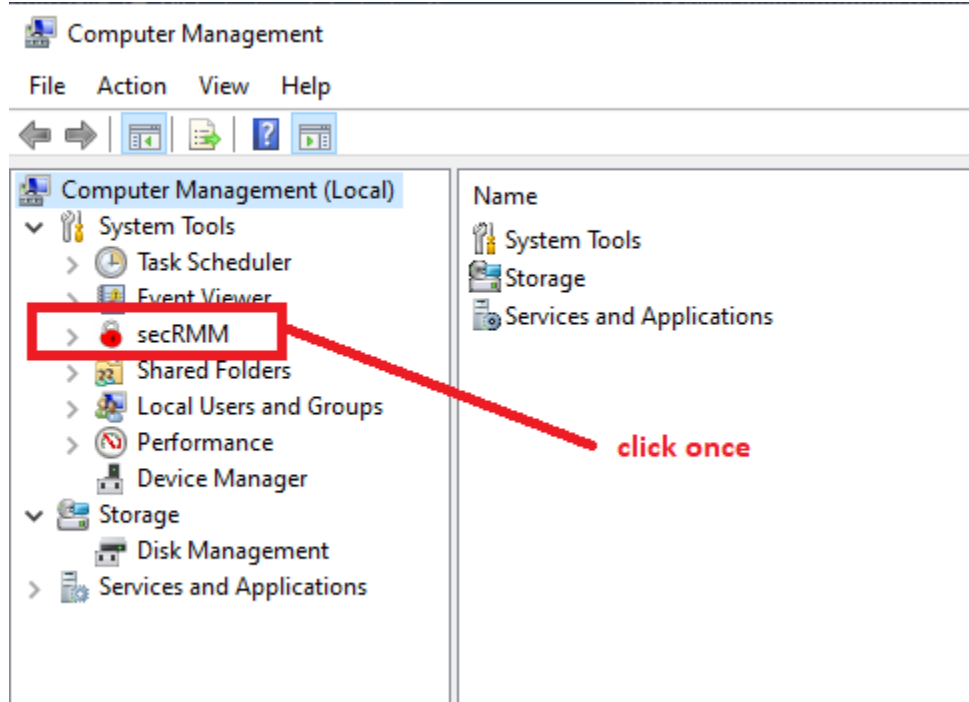
C:\Program Files\secRMM\AdminUtils\OpenDxl>
```

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.

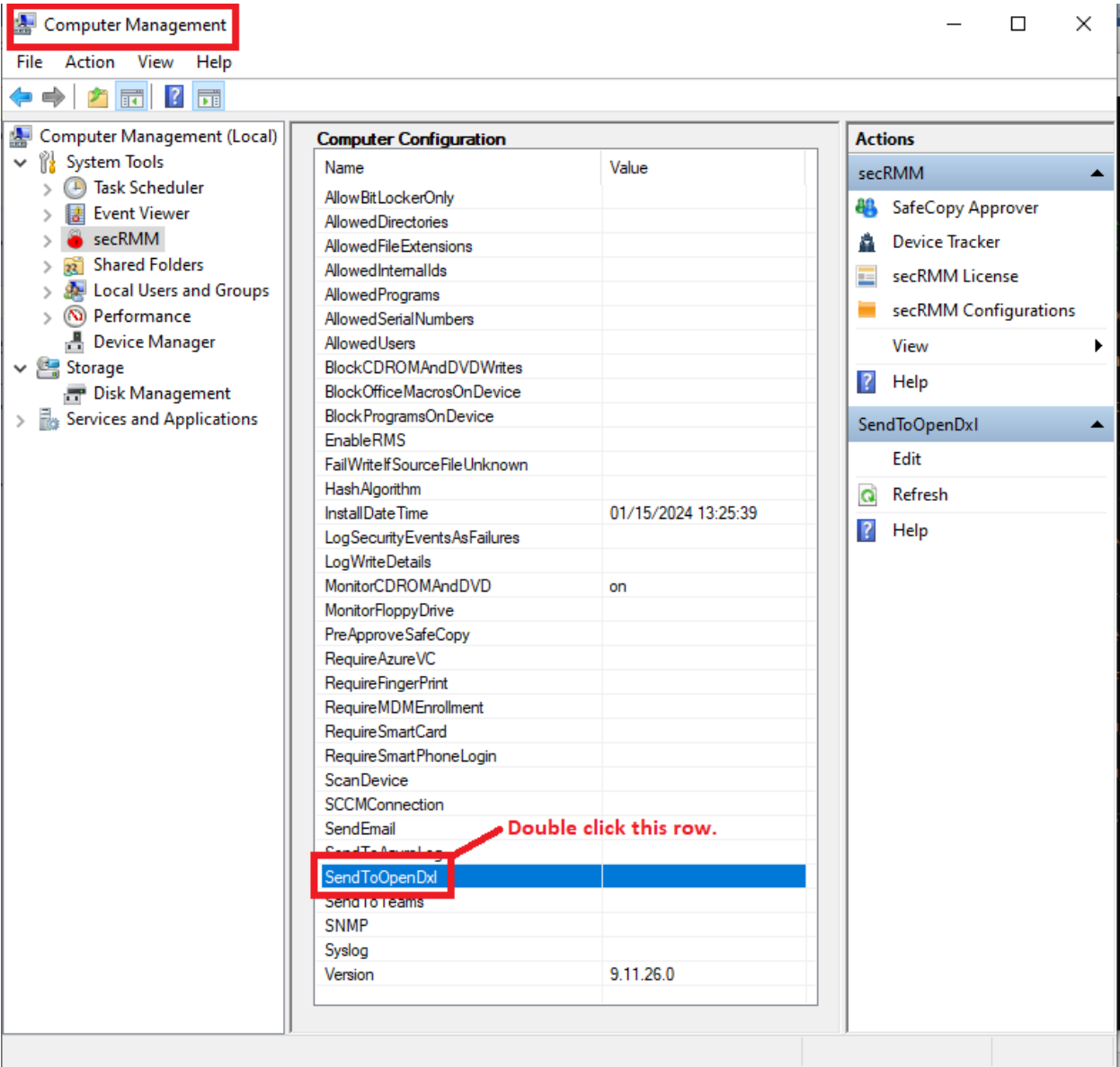
Configure secRMM to send security events to the OpenDxl fabric/servers

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.

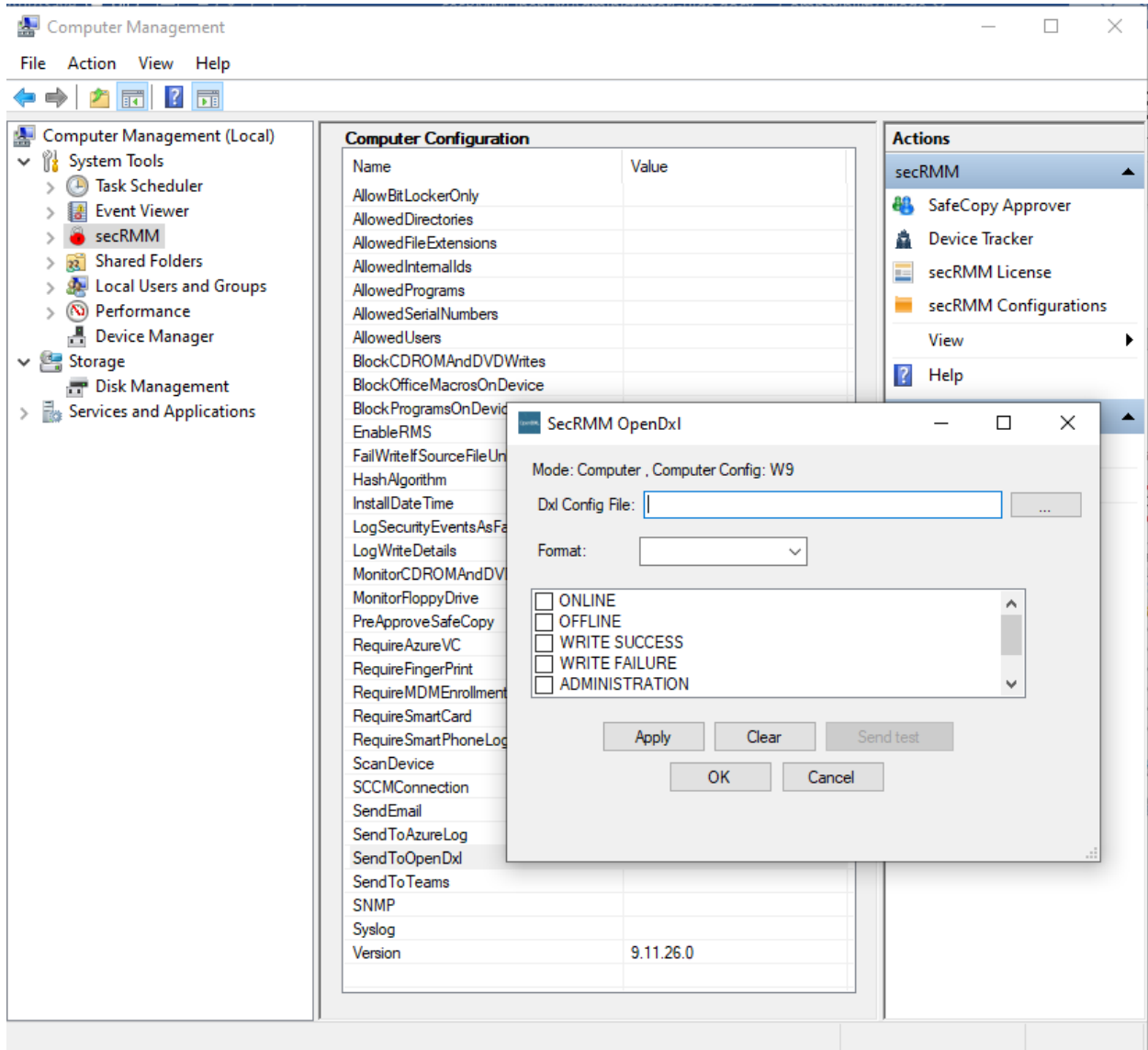




secRMM OpenDxl Administrator Guide



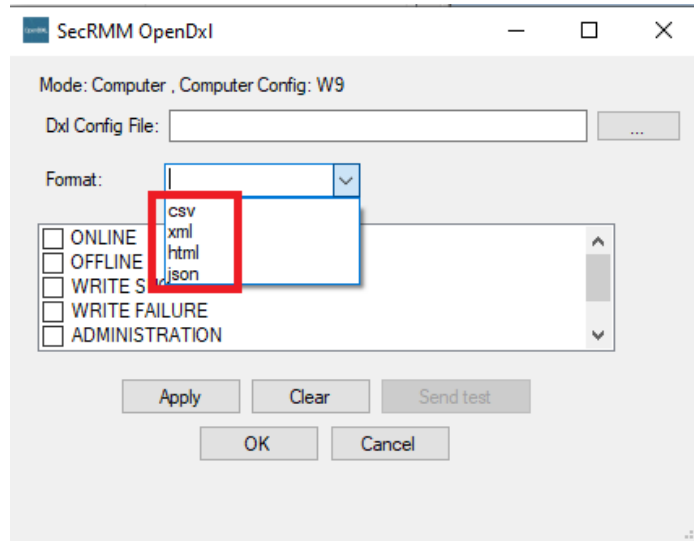
secRMM OpenDxl Administrator Guide



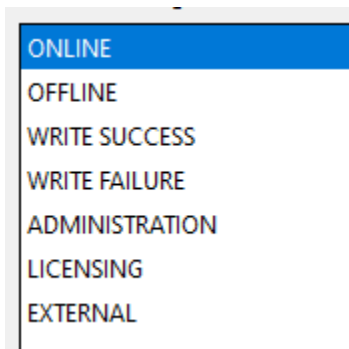
As you can see in the screenshot above, we need to supply 3 values to connect secRMM to the OpenDxl fabric/servers:

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 OpenDxl Administrator Guide



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:
- ONLINE
 - OFFLINE
 - WRITE SUCCESS
 - WRITE FAILURE
 - ADMINISTRATION
 - LICENSING
 - EXTERNAL

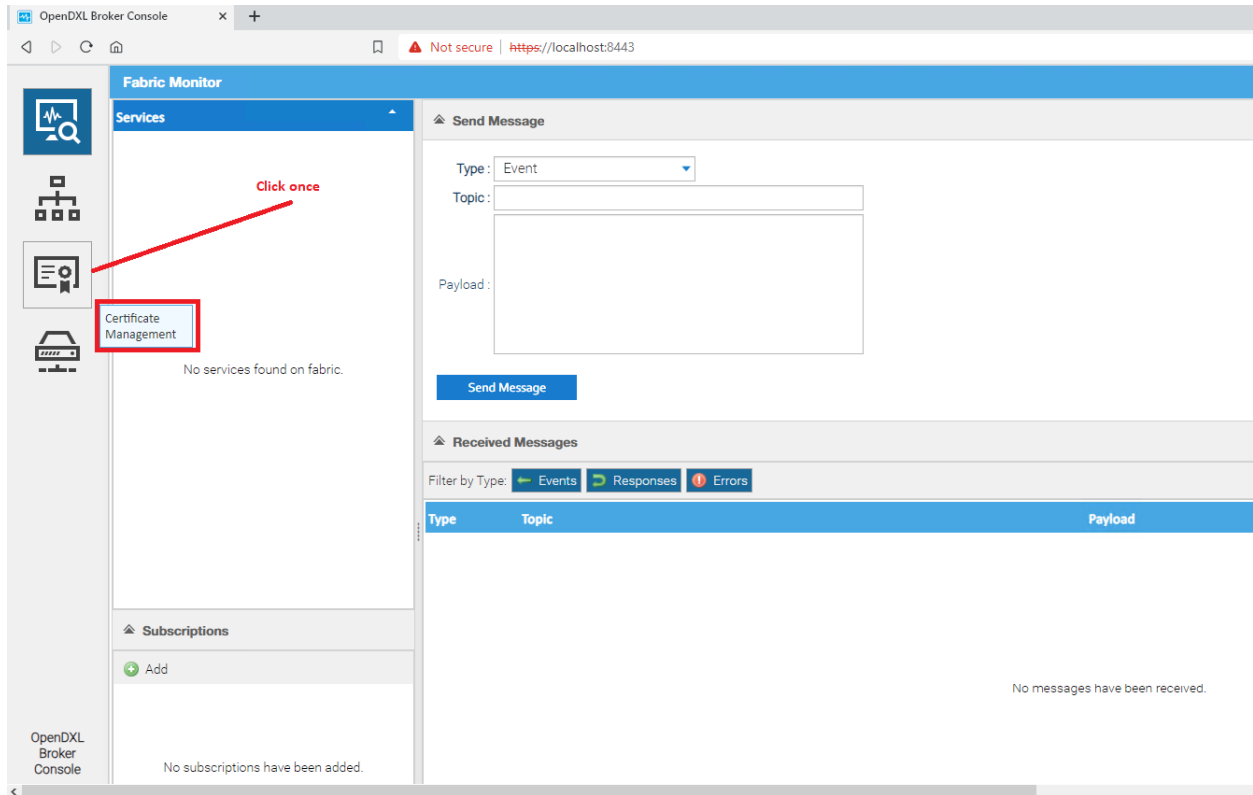


OpenDxl Configuration File

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.

secRMM OpenDxl Administrator Guide

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



Fill out this form and then click the generate button.

secRMM OpenDxl Administrator Guide

OpenDXL Broker Console

Not secure | <https://localhost:8443>

Generate Configuration

Configuration Type: Client Configuration

Common Name: (e.g. server FQDN or YOUR name)

Country Name: (2 letter code)

State or Province Name: (full name)

Locality Name: (eg, city)

Organization Name: (eg, company)

Organizational Unit Name: (eg, section)

Email Address:

Generate

OpenDXL Broker Console
Version: 0.3.3

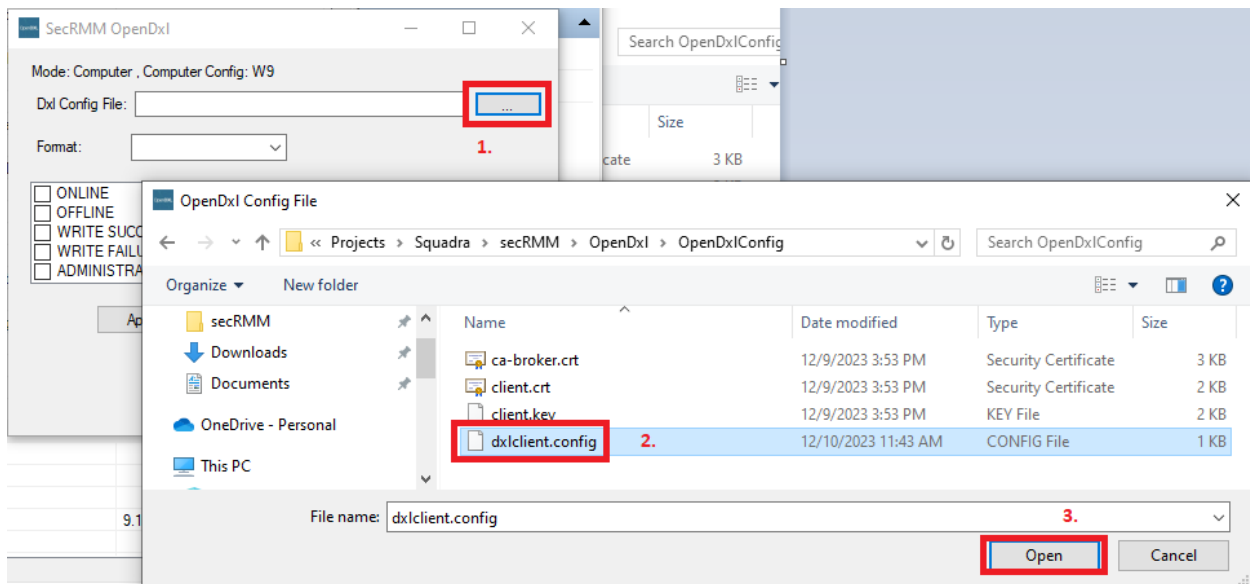
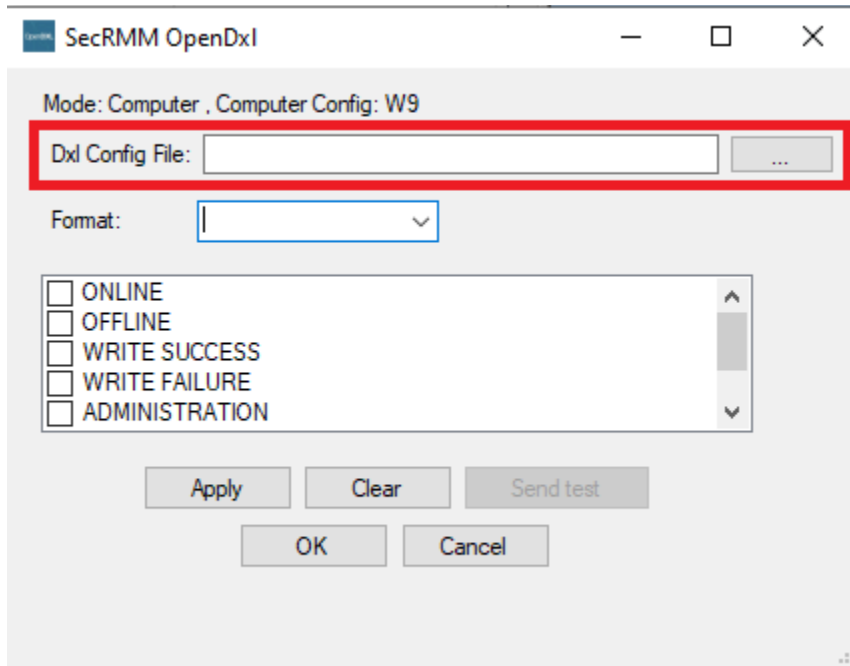
Logout

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

| Name | Date modified | Type | Size |
|------------------|---------------------|----------------------|------|
| ca-broker.crt | 12/9/2023 3:53 PM | Security Certificate | 3 KB |
| client.crt | 12/9/2023 3:53 PM | Security Certificate | 2 KB |
| client.key | 12/9/2023 3:53 PM | KEY File | 2 KB |
| dxlclient.config | 12/10/2023 11:43 AM | XML Configuratio... | 1 KB |

secRMM OpenDxl Administrator Guide

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

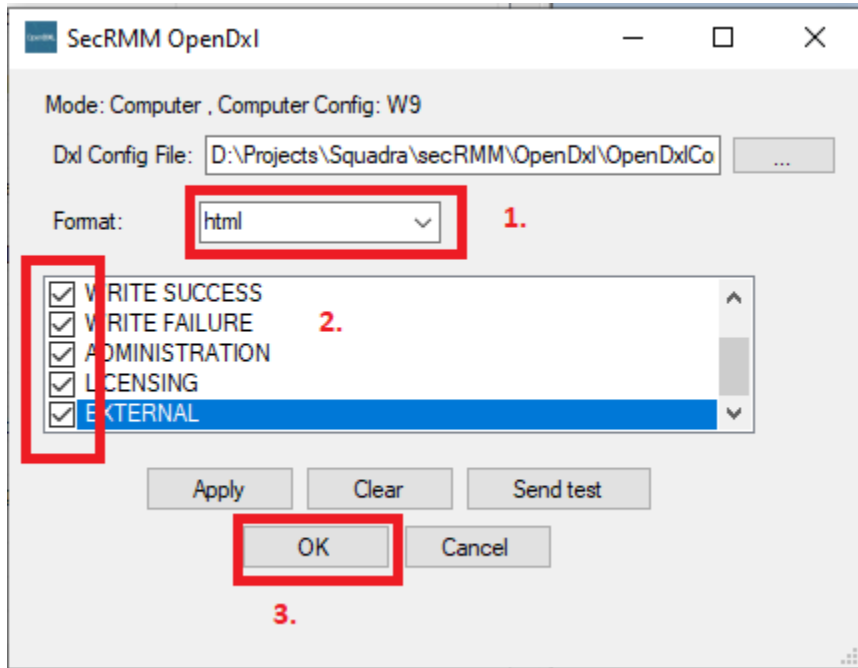


You might consider storing these 4 files on a network share and then specifying the network share when pointing secRMM to the dxlclient.config file. This has the advantage of having the files in one spot and not replicated. However, the disadvantage is that the network share would need to be online when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

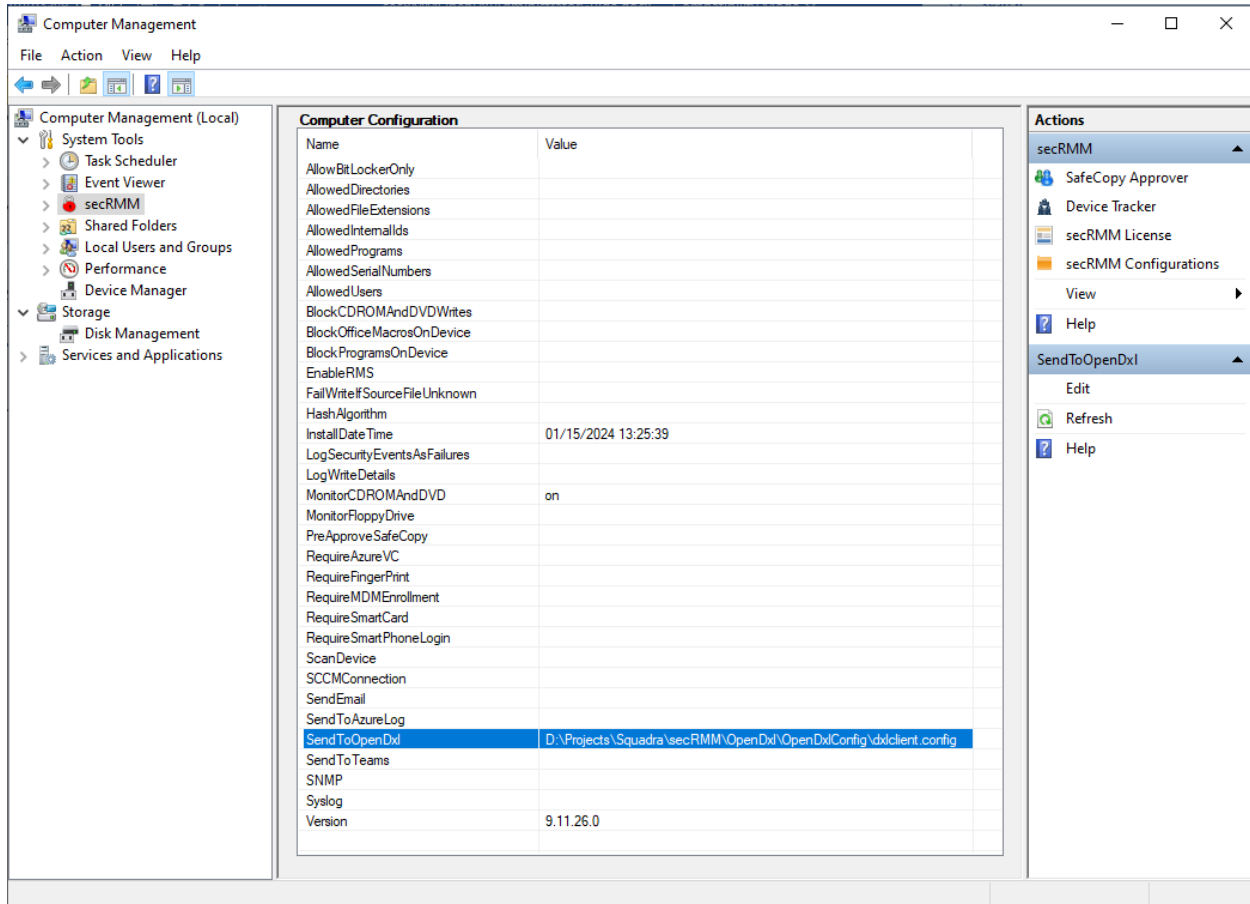
secRMM OpenDxl Administrator Guide

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 OpenDxl Administrator Guide

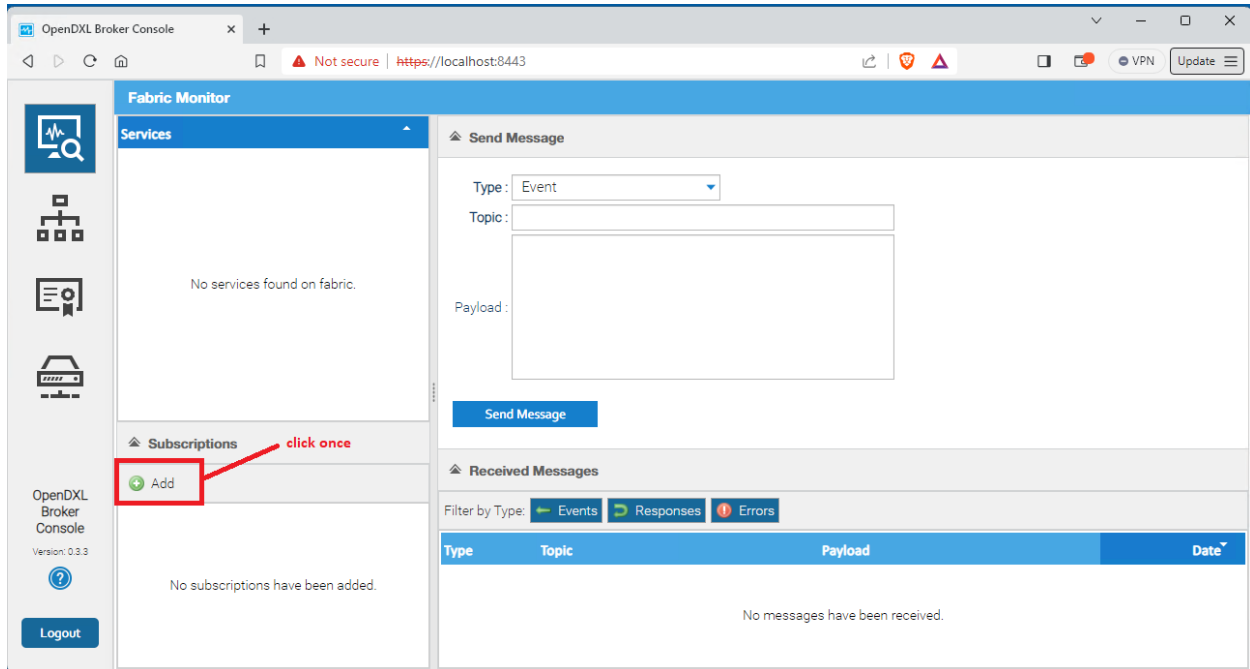


Configure the OpenDxl fabric/servers to receive secRMM events

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.

secRMM OpenDxl Administrator Guide



In the entry field, type:

/secRMM

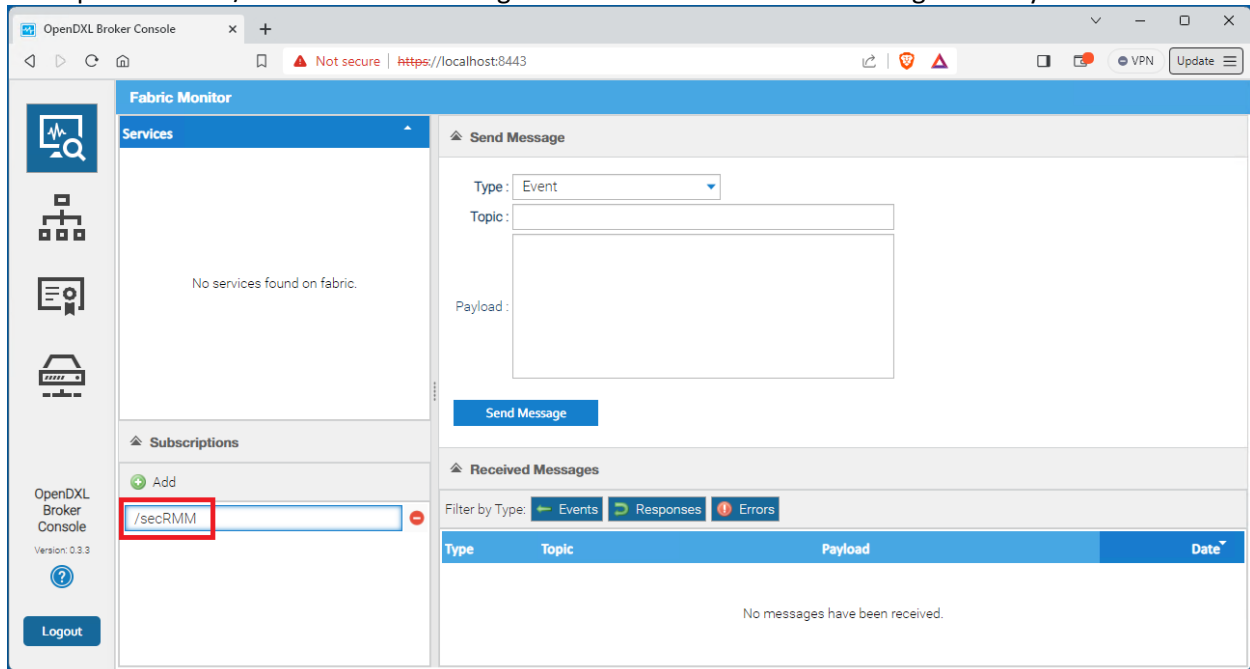
Don't forget the forward slash (/) as the first character.

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).

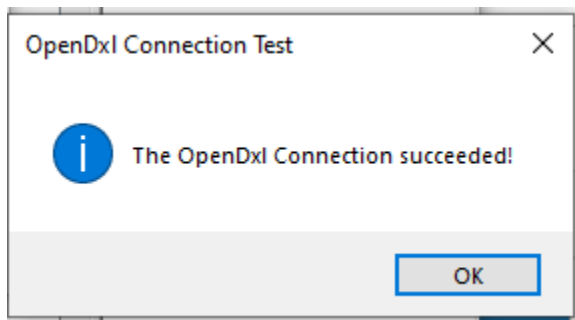
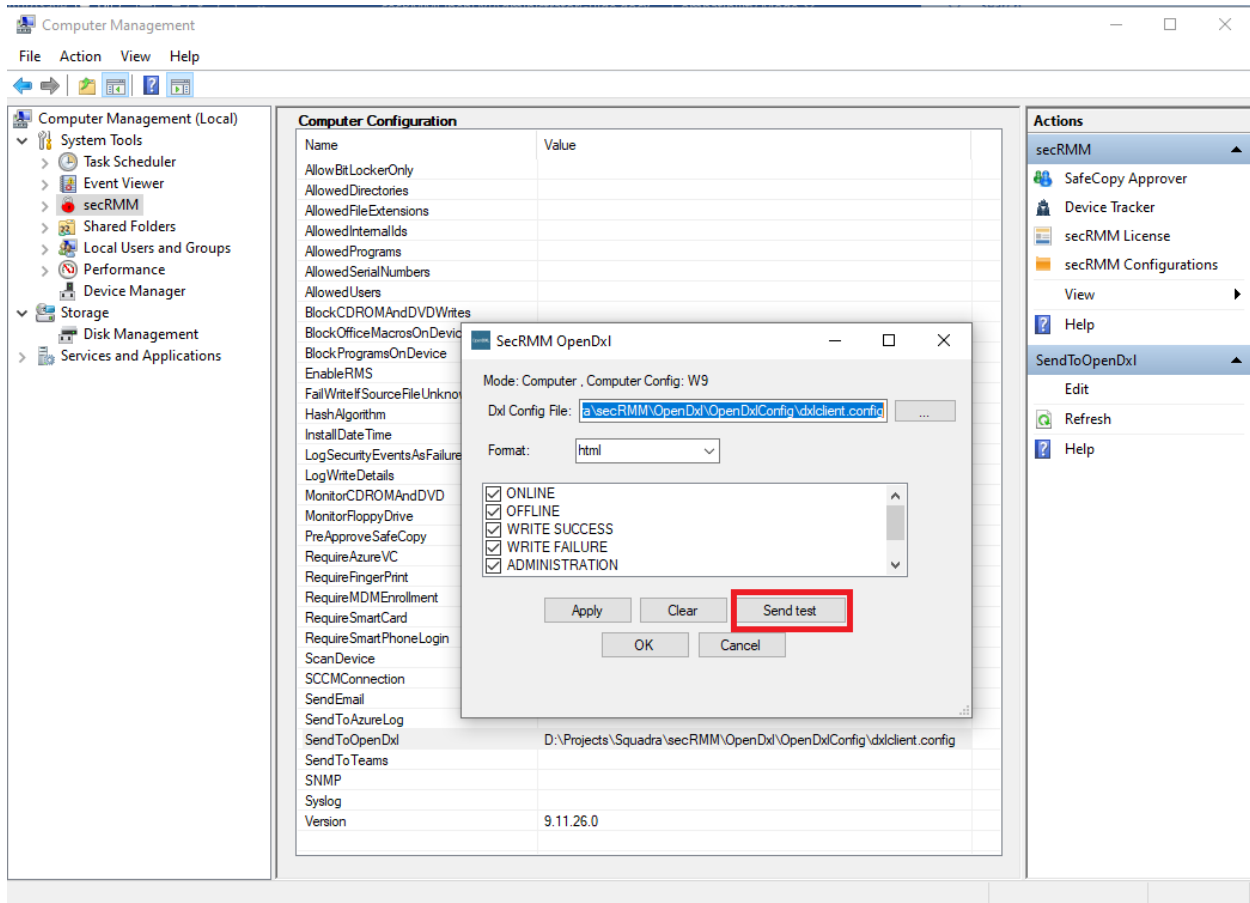
The OpenDxl fabric/server is now listening for the secRMM removable storage security events



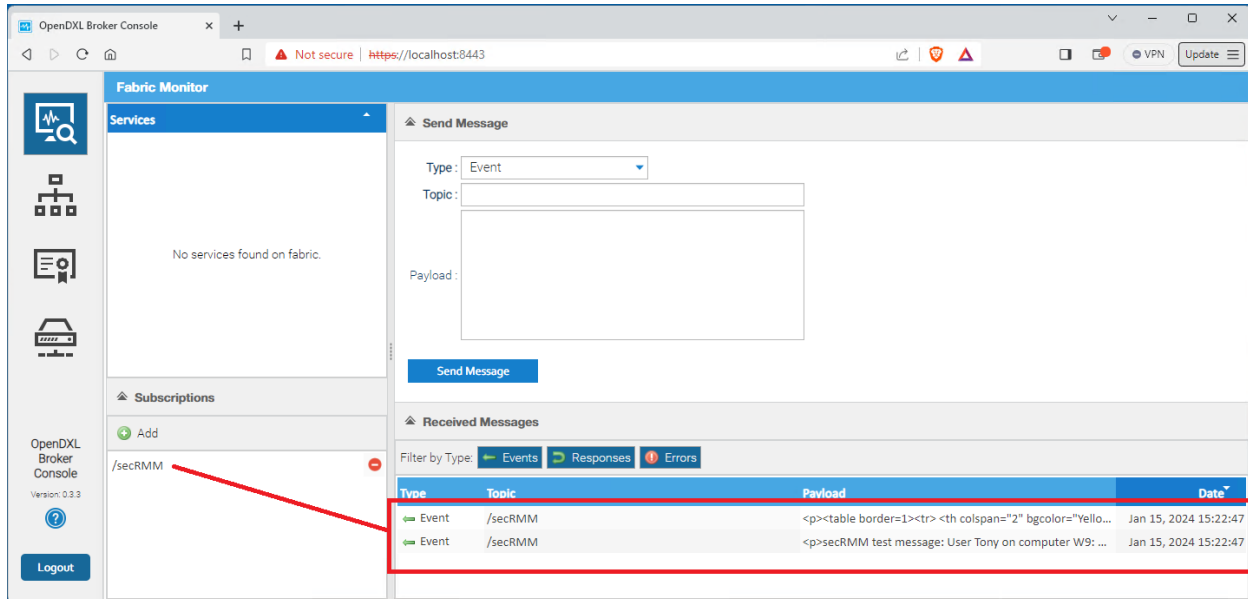
secRMM OpenDxl Administrator Guide

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

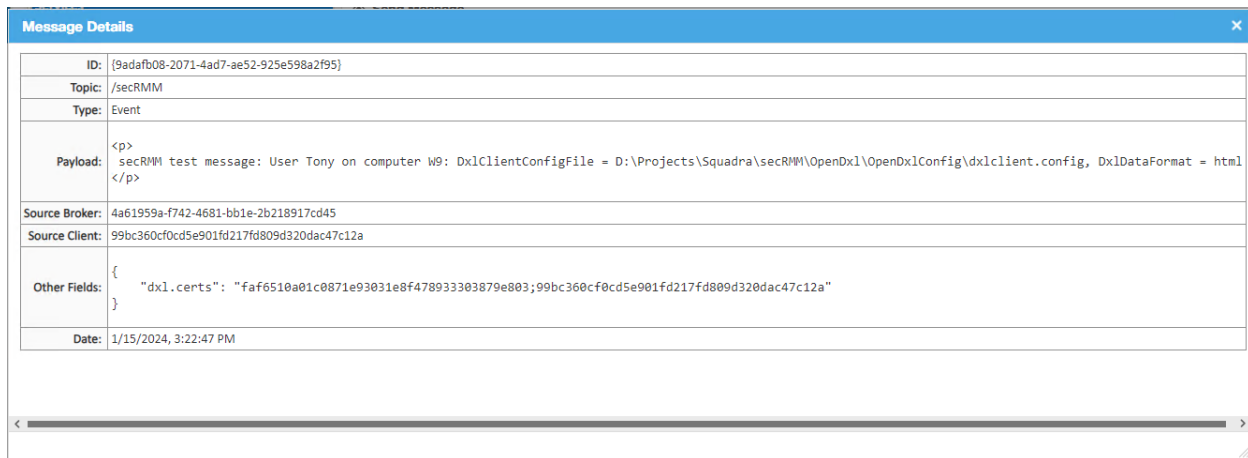
Once you have completed the above configuration steps, you can test the secRMM connection to the OpenDxl fabric/servers using the Windows Computer Management tool.



secRMM OpenDxl Administrator Guide



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!



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/ |