

nox medical



IMPLEMENTING NOX MEDICAL PRODUCT IN SECURITY POLICIES

Pedro Nogueira
Nox Medical

What is GDPR

The General Data Protection Regulation (GDPR), is a new set of data privacy laws that require businesses to prioritize the protection and privacy of personal data belonging to European Union (EU) residents.

The purpose of this presentation is to outline how Nox Medical's products can be implemented in security policies within organizations.

Security policies are implemented within most organizations and this document will help IT to understand how Nox Medical's products impact their policies.

Overview

Nox Recorders

The Nox T3 and the Nox A1 (Nox Recorders) store patient data on the device. When a sleep study is prepared, there is patient demographic information (name etc.) stored on the Nox Recorder. The recorder stores the data in an encrypted form.

Nox C1 Access Point

The Nox C1 is a network access point which does not store any data.

Noxturnal

Noxturnal is the analysis software needed to view and score the physiological signals recorded with the Nox recorders.

Windows Security Policies

Noxturnal software is not a native database.

Users can configure Windows to know who has accessed and changed patient information.

This is done through the organization's security policy and Windows Domain Controller

Key elements of such a policy are:

- No shared access, logins or passwords on any computer.
- Each user must have a unique login and secret password when working on a computer belonging to the organization.

Implementing Nox Medical Products in Security Policies

The purpose of this memo is to outline how Nox Medical's products can be implemented in security policies within organizations. Security policies are implemented within most organizations and this document will help IT to understand how Nox Medical's products impact their policies.

It is important that an organization must take a holistic view of implementing security policies and standards. Single products cannot make organizations compliant. Instead – they should fit within the realm of organization-wide policies.

Please download the memo and toolkit below.

*Please note that not all features or all products are available in all markets. Our products are medical devices and subject to registration/approval in each market area. For more information on product availability please contact support@noxmedical.com






April 29, 2019 11:55



- [Implementing Nox Medical Products in Security Policies.pdf \(300 KB\)](#)
- [Nox Security Helper Toolkit - Workstations.zip \(10 KB\)](#)
- [Nox Security Helper Toolkit - Server.zip \(20 KB\)](#)

Configuration Standalone Workstation

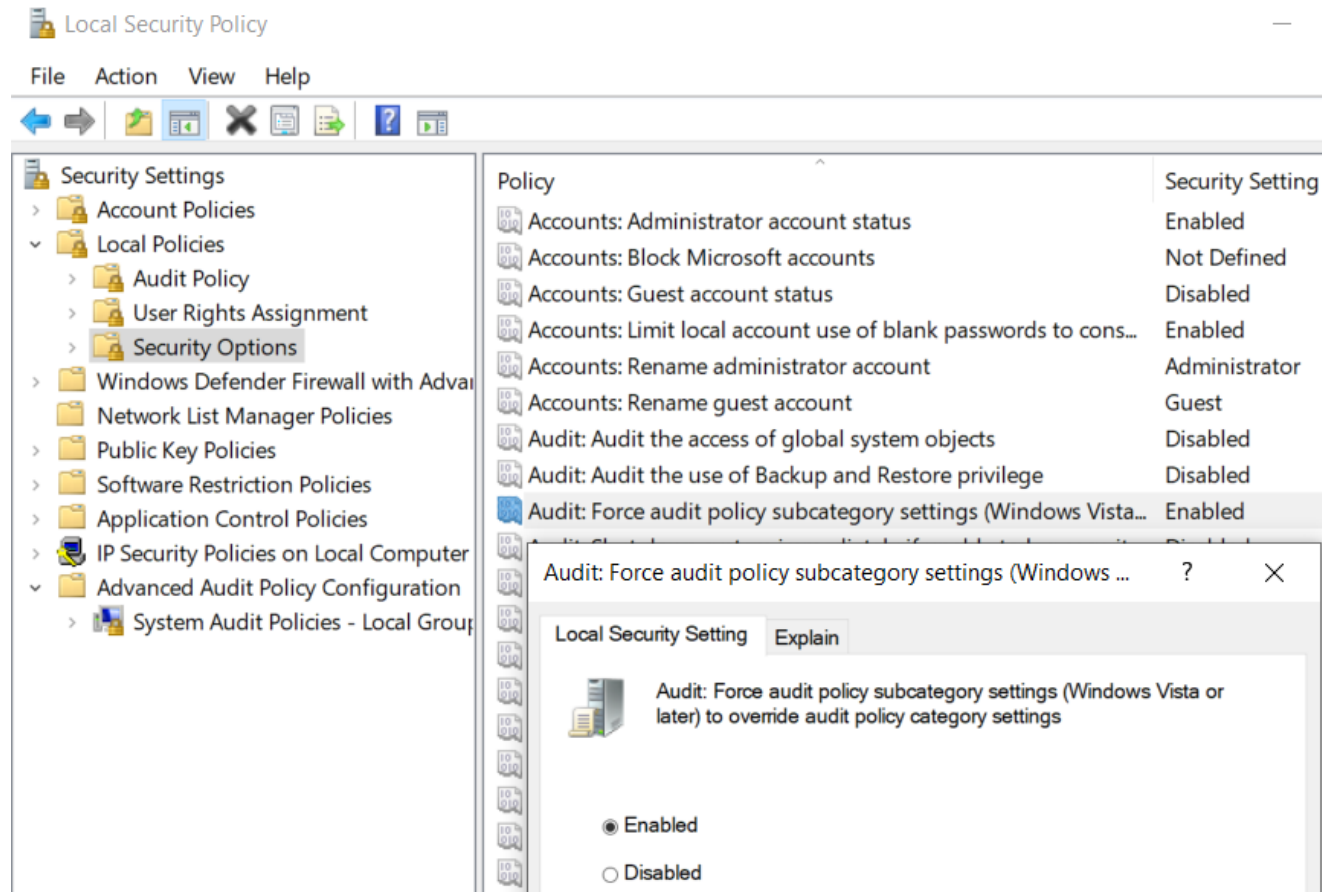
1.) Download and unzip the files found on Nox Medical's website under "Implementing Nox Medical Products in Security Policies", including these instructions.

Name	Date modified	Type	Size
 Implementing Nox Medical Products in Security Policies	03-Sep-19 12:50	Adobe Acrobat D...	245 KB
 Nox Security Helper Toolkit - Server	02-Sep-19 14:52	Compressed (zipp...	22 KB
 Nox Security Helper Toolkit - Workstations	02-Sep-19 14:50	Compressed (zipp...	11 KB

2.) Enable Advanced Policies in Local Security Settings

- Open Control Panel
 - System and Security
 - Administrative Tools
 - Local Security Policy

- In Security Options under Local Policies open the "Audit: Force audit policy subcategory settings" and select "Enabled"



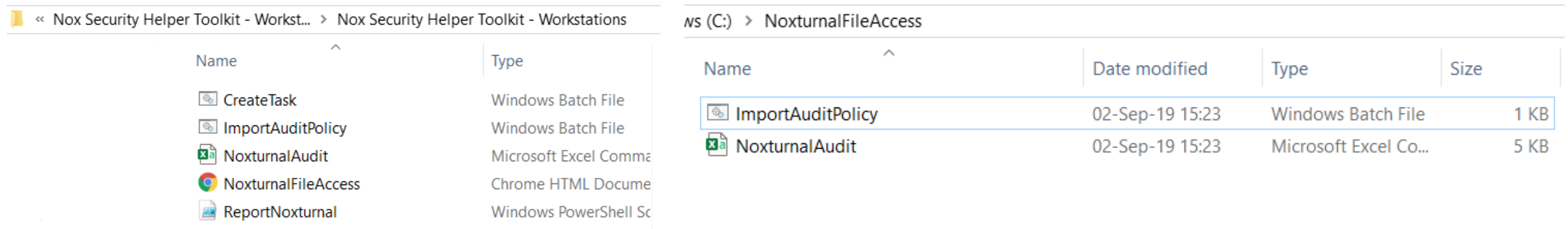
The screenshot shows the Windows Local Security Policy console. The left pane displays a tree view of security settings, with 'Security Options' under 'Local Policies' selected. The right pane shows a list of policies, with 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' highlighted. A dialog box is open for this policy, showing the 'Local Security Setting' tab with the 'Enabled' radio button selected.

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to cons...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vista...	Enabled

Configuration Standalone Workstation

3.) Create the folder to be used for data collection “C:\NoxturnalFileAccess”

Extract NoxturnalAudit.csv and ImportAuditPolicy.bat to C:\NoxturnalFileAccess folder.



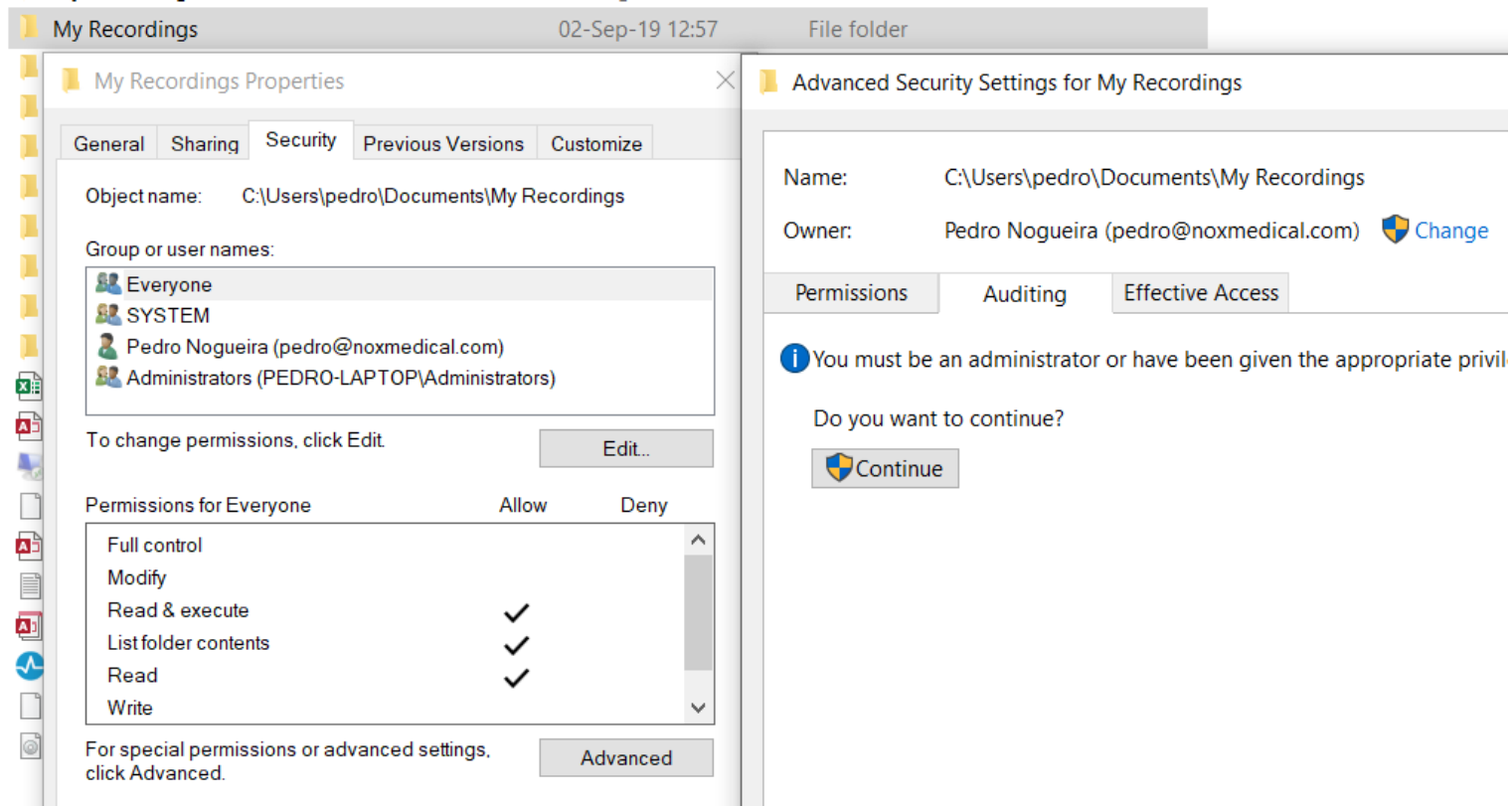
4.) Right click the ImportAuditPolicy.bat file and click “Run as Administrator”.

The Audit Policies have now been applied

Configuration Standalone Workstation

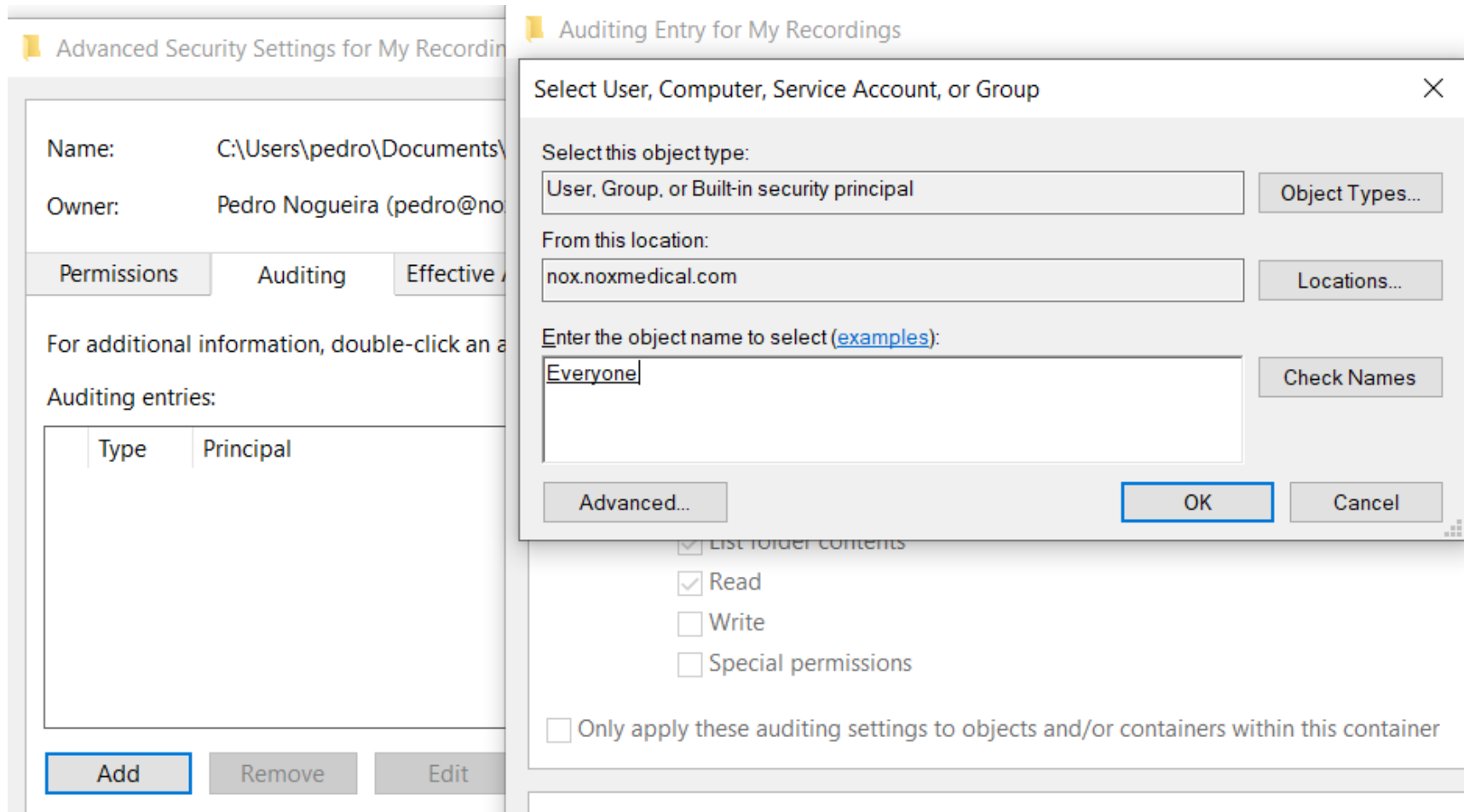
5.) Assigning File Audit Permissions to the Noxturnal Data Folder (The folder with Sleep Recordings)

Right Click the Noxturnal Folder -> Properties -> Security Tab -> Advanced -> Auditing Tab -> Continue



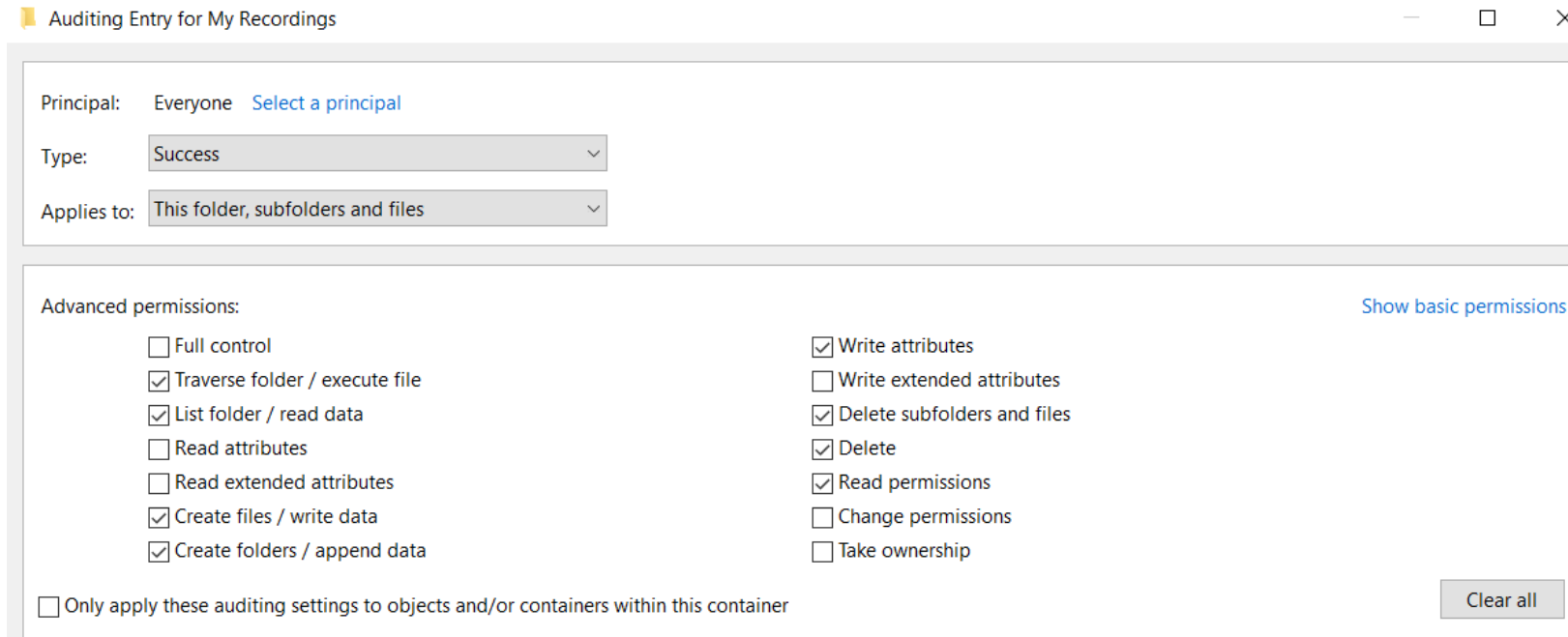
Configuration Standalone Workstation

6.) Click Add and create "Everyone"



Configuration Standalone Workstation

7.) Select “Show advanced Permissions”



The screenshot shows the 'Auditing Entry for My Recordings' dialog box. The 'Principal' is set to 'Everyone' with a 'Select a principal' link. The 'Type' is set to 'Success' and 'Applies to' is set to 'This folder, subfolders and files'. The 'Advanced permissions' section is expanded, showing a list of permissions with checkboxes. The checked permissions are: Traverse folder / execute file, List folder / read data, Create files / write data, Create folders / append data, Write attributes, Delete subfolders and files, Delete, and Read permissions. There is a 'Show basic permissions' link and a 'Clear all' button.

Auditing Entry for My Recordings

Principal: Everyone [Select a principal](#)

Type: Success

Applies to: This folder, subfolders and files

Advanced permissions: [Show basic permissions](#)

<input type="checkbox"/> Full control	<input checked="" type="checkbox"/> Write attributes
<input checked="" type="checkbox"/> Traverse folder / execute file	<input type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input checked="" type="checkbox"/> Delete subfolders and files
<input type="checkbox"/> Read attributes	<input checked="" type="checkbox"/> Delete
<input type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input checked="" type="checkbox"/> Create files / write data	<input type="checkbox"/> Change permissions
<input checked="" type="checkbox"/> Create folders / append data	<input type="checkbox"/> Take ownership

Only apply these auditing settings to objects and/or containers within this container

Clear all

Add the following ACL with checkboxes checked

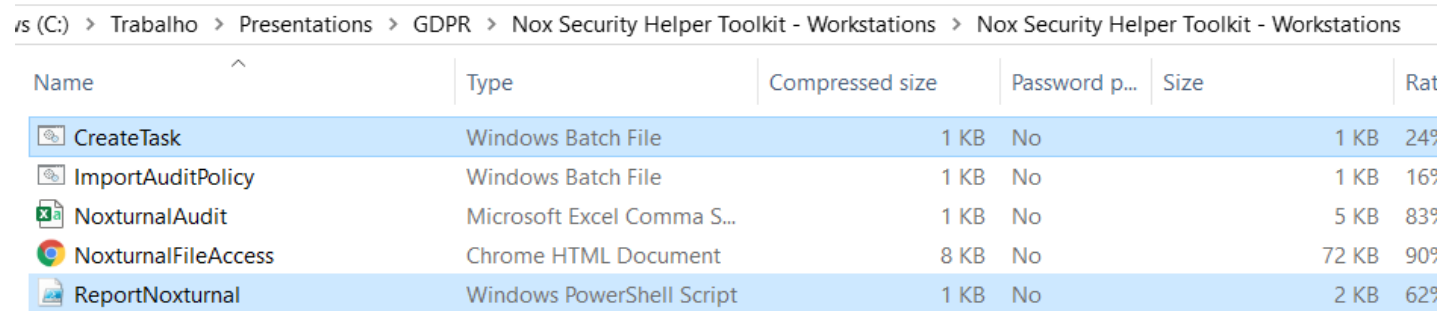
- List folder / read data
- Create files / write data
- Create folders / append data
- Delete subfolder and files
- Delete

The File Audit ACL's are now set and Security EventLog is recording all file read and write access.

Configuration Standalone Workstation

8.) Adjust script configuration and setup Scheduled Task

Unzip the ReportNoxturnal.ps1 script file and CreateTask.bat to C:\NoxturnalFileAccess folder



Name	Type	Compressed size	Password p...	Size	Rat
CreateTask	Windows Batch File	1 KB	No	1 KB	24%
ImportAuditPolicy	Windows Batch File	1 KB	No	1 KB	16%
NoxturnalAudit	Microsoft Excel Comma S...	1 KB	No	5 KB	83%
NoxturnalFileAccess	Chrome HTML Document	8 KB	No	72 KB	90%
ReportNoxturnal	Windows PowerShell Script	1 KB	No	2 KB	62%

If studies are being saved in a file server:

Edit the C:\NoxturnalFileAccess\ReportNoxturnal.ps1 and set the \$server variable.

If running the script on the fileserver \$server should be unset.

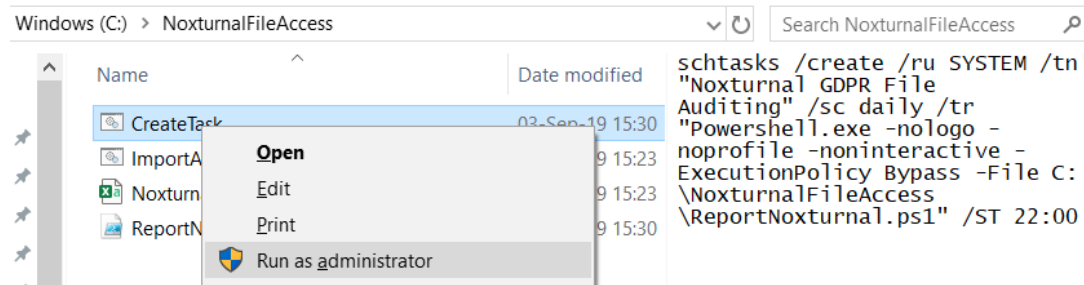
Adjust CSVFile according to needs.

```
ReportNoxturnal.ps1 X
1 #
2 # PowerShell - Nox Medical
3 #
4
5 # Use Servername only if running from remote Server
6 # $server = "FileServer01"
7 $server = ""
8
9 # Path to Audit Log CSV File
10 $CSVFile = "c:\NoxturnalFileAccess\audit.csv"
11
12 # Days To Scan Security Events. Usually 1 Day
13 $TimeSpan = 1;
14
15 # $server = @f
```

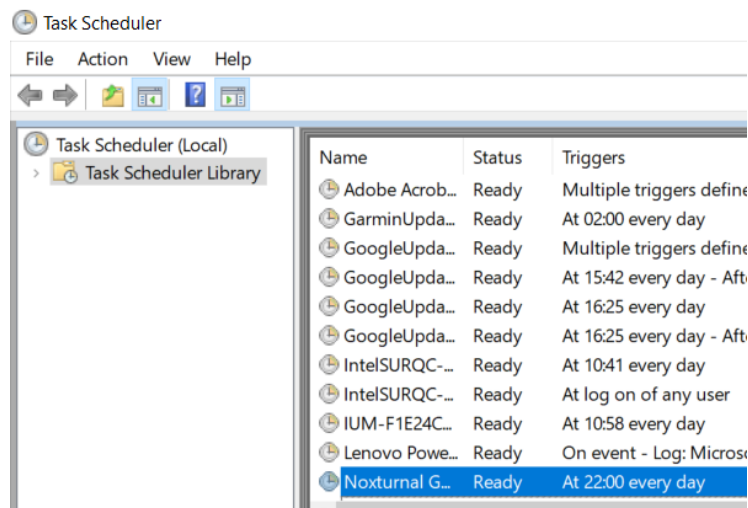
Configuration Standalone Workstation

9.) Create a Scheduled Task

Right click the CreateTask.bat and select „Run As Administrator“.



This will create a task named "Noxturnal File Auditing" and can be modified in Task Scheduler to run at the desired hour of day.



The CSV File will now append file access data once daily for later processing with Excel or SQL database.

Configuration Standalone Workstation

The task named Noxturnal File Auditing can be modified by accessing properties.
Importante to confirm / adjust the Conditions and Settings

The image displays three overlapping screenshots of the Windows Task Scheduler 'Noxturnal GDPR File Auditing Properties' dialog box, illustrating the configuration process.

Top Screenshot (Triggers Tab): Shows the 'Triggers' tab with a table of triggers. The table has columns for 'Trigger', 'Details', and 'Status'. A single trigger is listed: 'Daily' with details 'At 22:00 every day' and status 'Enabled'. Below the table are buttons for 'New...', 'Edit...', and 'Delete'. At the bottom right are 'OK' and 'Cancel' buttons.

Trigger	Details	Status
Daily	At 22:00 every day	Enabled

Middle Screenshot (Conditions Tab): Shows the 'Conditions' tab with the instruction: 'Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.' The 'Idle' section includes:

- Start the task only if the computer is idle for: 10 minutes (dropdown)
- Wait for idle for: 1 hour (dropdown)
- Stop if the computer ceases to be idle
- Restart if the idle state resumes

The 'Power' section includes:

- Start the task only if the computer is on AC power
- Stop if the computer switches to battery power

The 'Network' section includes:

- Wake the computer to run this task
- Start only if the following network connection is available: Any connection (dropdown)

'OK' and 'Cancel' buttons are at the bottom right.

Bottom Screenshot (Settings Tab): Shows the 'Settings' tab with the instruction: 'Specify additional settings that affect the behavior of the task.' The settings include:

- Allow task to be run on demand
- Run task as soon as possible after a scheduled start is missed
- If the task fails, restart every: 1 minute (dropdown)
- Attempt to restart up to: 3 times
- Stop the task if it runs longer than: 3 days (dropdown)
- If the running task does not end when requested, force it to stop
- If the task is not scheduled to run again, delete it after: 30 days (dropdown)
- If the task is already running, then the following rule applies: Do not start a new instance (dropdown)

'OK' and 'Cancel' buttons are at the bottom right.

nox medical



THANK YOU