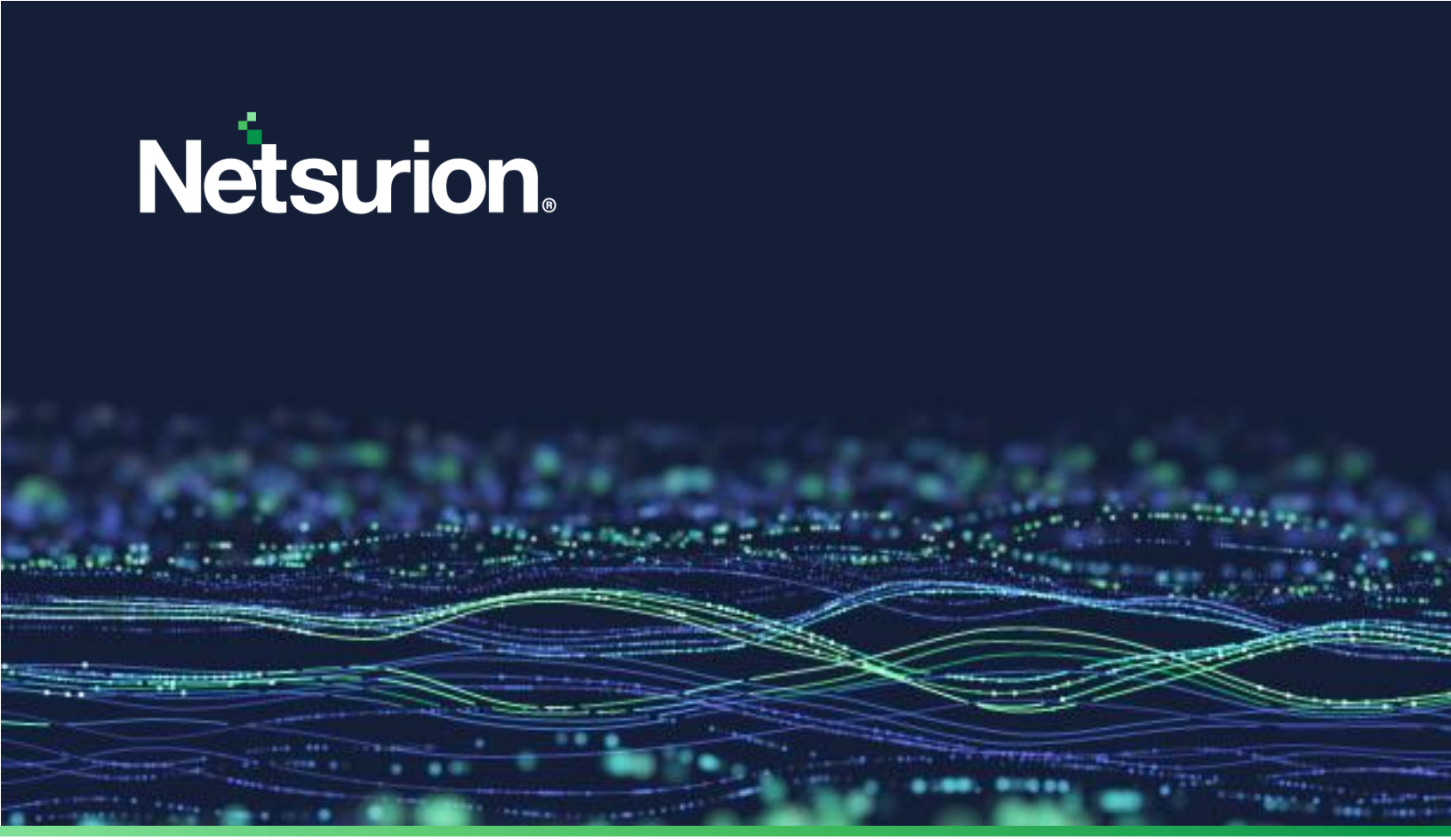


Quick Reference Guide

Configure Advanced Audit Policy for Windows

Publication Date:

June 22, 2023

Abstract

This document describes the security audit policy settings available in Windows Server 2008 onwards , Windows 7 onwards, and audit events that they generate.

These settings allow selecting only the behavior you want to monitor and excludes audit results for other behaviors. In addition, security audit policies can be applied by using domain group policy, audit policy settings can be modified, tested, and deployed to selected users and groups.

Refer to Windows Advanced Audit Policy Configuration to know more about Windows Advanced Audit Policy Configuration.

Scope

The configuration details in this guide are consistent with Netsurion Open XDR 9.3 or later.

Audience

Netsurion Open XDR users responsible for investigating and managing network security.

Table of Contents

1 Account Logon

Account Logon		
Audit Credential Validation	Enable	Enable
Kerberos Authentication Service	Enable	Enable
Account Logon-Audit Kerberos Service Ticket Operations	Enable	Enable
Audit Other Account Logon Events	Enable	Enable

2 Account Management

Account Management		
Application Group Management	Enable	Enable
Computer Account Management	Enable	Enable
Distribution Group Management	Enable	Enable
Audit Other Account Management Events	Enable	Enable
Security Group Management	Enable	Enable
User Account Management	Enable	Enable

3 Detailed Tracking

Detailed Tracking		
DPAPI Activity	Disable	Disable
Process Creation	Enable	Enable
Process Termination	Enable	Enable
RPC Events	Enable	Enable

4 DS Access

DS Access		
Detailed Directory Service Replication	Disable	Disable
Directory Service Access	Enable	Enable
Directory Service Changes	Enable	Enable
Directory Service Replication	Disable	Disable

5 Logon / Logoff

Logon / Logoff		
Account Lockout	Enable	Enable
IPsec Extended Mode	Disable	Disable
IPsec Main Mode	Disable	Disable
IPsec Quick Mode	Disable	Disable
Account Logoff	Enable	Enable
Account Logon	Enable	Enable
Network Policy Server (NPS)	Enable	Enable
Other Logon/Logoff Events	Enable	Enable
Special Logon	Enable	Enable

6 Object Access

Object Access		
Application Generated	Enable	Enable
Certification Services	Enable	Enable
Detailed File Share	Disable	Disable
File Share	Enable	Enable
File System	Enable	Enable
Filtering Platform	Disable	Disable
Filtering Platform Packet Drop	Disable	Disable
Handle Manipulation	Disable	Disable
Kernel Object	Enable	Enable
Other Object Access Events	Optional*	Optional *

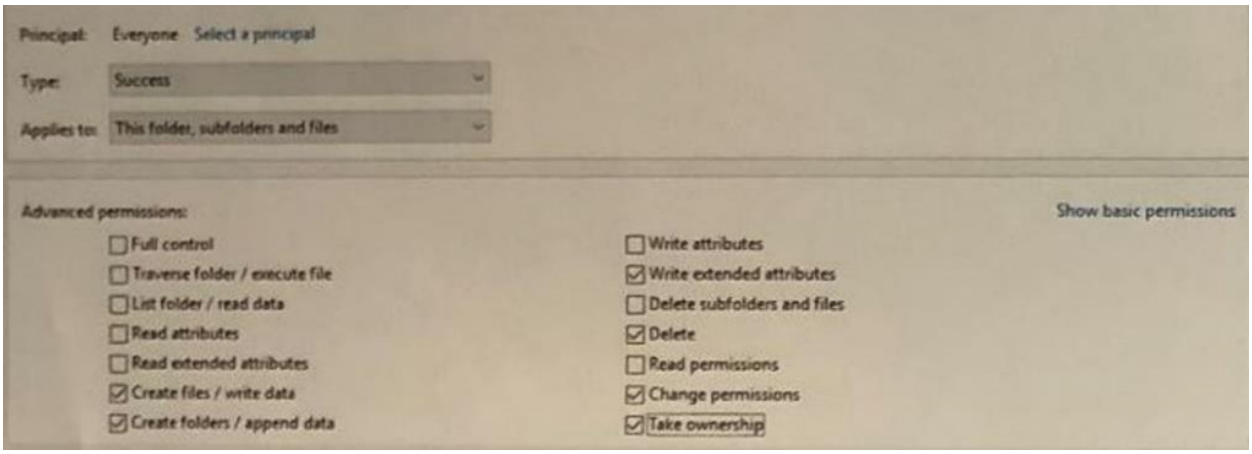
Object Access		
Registry	Enable	Enable
SAM-Security Accounts Manager	Disable	Disable

*If you choose to track Scheduled Tasks through auditing, you can turn this Audit Sub Category on.

6.1 Configuration

These are the recommended settings to optimize what is needed security-wise and to minimize the noise.

1. Select the folder or file you wish to audit. Right-click the folder, select **Properties**, and navigate to the **Security** tab. Click the **Advanced** button.
2. Navigate to the **Auditing** tab and click the **Add** button. Provide values as given below:
    - Principal: “EveryOne”
    - Type: “Success”
    - Applies to: “THIS FOLDER and FILES” or “ THIS FOLDER, SUBFOLDERS and FILES”
3. Click **Show advanced permissions** and select only:
    - Create files/write data
    - Create folders/append data
    - Write extended attributes
    - Delete
    - Change permissions
    - Take ownership to audit
4. Click **OK**.



6.2 Recommended folders to audit

THIS FOLDER AND FILES ONLY	THIS FOLDER,SUBFOLDERS AND FILES
Auditing of the subfolder(s) is not recommended	C:\Boot
C:\Program Files	C:\Perflogs
C:\Program Files\Internet Explorer	Any Anti-Virus folder(s) used for quarantine, etc.
C:\Program Files\Common Files	C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Startup
C:\Program Files (x86)	C:\Users\Public
C:\Program Files (x86)\Common Files	C:\Users*\AppData\Local
C:\ProgramData	C:\Users*\AppData\LocalLow
C:\Windows	C:\Users*\AppData\Roaming
C:\Windows\System32	C:\Windows\Scripts
C:\Windows\System32\Drivers	C:\Windows\System
C:\Windows\System32\Drivers\etc	C:\Windows\System32\GroupPolicy\Machine\ Scripts
C:\Windows\System32\Sysprep	C:\Windows\System32\GroupPolicy\User\ Scripts
C:\Windows\System32\wbem	C:\Windows\System32\Repl (only on servers)
C:\Windows\System32\WindowsPoweShell\v1.0	
C:\Windows\Web	
C:\Windows\SysWOW64	
C:\Windows\SysWOW64\Drivers	
C:\Windows\SysWOW64\wbem	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0	

Files are often added or changed by hackers and malware. By auditing key file and folder locations, any additions or changes made by an attacker can be captured in the logs, which is beneficial for alerting and forensics.

6.3 Excluded folders from Auditing

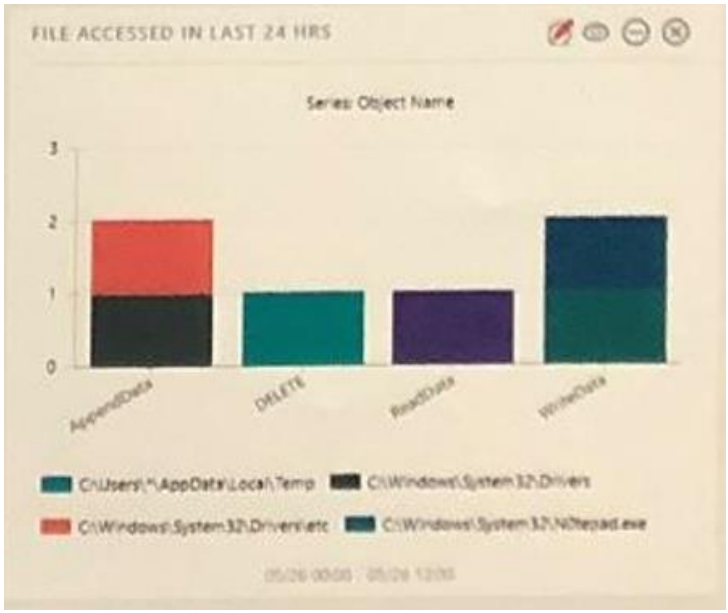
After setting auditing on the parent folder, remove auditing from these folders to reduce the noise events.

THIS FOLDER AND FILES ONLY	THIS FOLDER,SUBFOLDERS AND FILES
C:\ProgramData\Microsoft\RAC\Temp	C:\Users*\AppData\Local\Microsoft\Windows\Explorer\thumbcache_*
C:\ProgramData\Microsoft\RAC\PublishedData\RacWmiDatabase.sdf	C:\Users*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
C:\ProgramData\Microsoft\RAC\StateData\RacDatabase.sdf	C:\Users*\AppData\Local\Microsoft\Office
C:\ProgramData\<Anti-Virus>\CommonFramework Insert your AV folder(s)	C:\Users*\AppData\Local\Microsoft\Outlook
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.chk	C:\Users*\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.log	C:\Users*\AppData\Local\Microsoft\Mozilla\Firefox\Profiles
C:\ProgramData\Microsoft\Windows\WER\Temp\	C:\Users*\AppData\LocalLow\Microsoft\Cryptnet UrlCache
C:\ProgramData\Microsoft\Diagnosis	C:\Users*\AppData\Roaming\Microsoft\Excel
C:\Users*\AppData\Local\GDIPFONTCACHEV1.DAT	C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\ CryptnetUrlCache
C:\Users*\AppData\Local\Google\Chrome\User Data	

Any other folder which might result in generating large noise events.

6.4 Visualization

Changes to the monitored folder/file results in the generation of a security log with Event ID 4663 that contains the change details. Using this event, you can generate alert or visualize the data through dashboards and reports.



Windows-Local file or resource access details

LogTime	Computer	User Name	User Domain	Process Name	Object Path	Access Details
05/26/2017 11:09:26 AM	Contoso-mktwks	James	CONTOSO	C:\user\james\appdata\temp\Microsoft\Office16\word.exe	d:\data\employee\confidential files\Payroll.xlsx	ReadData
05/26/2017 02:52:48 AM	Contoso-DNSSrv	Mike	CONTOSO	C:\Windows\Roaming.exe	C:\Windows\System32\Drivers\etc\hosts	AppendData
05/23/2017 06:45:48 AM	Contoso-DNSSrv	Mike	CONTOSO	C:\Program Files\DNS\dnssvc.exe	C:\Windows\System32\Drivers\etc\lmhost	AppendData
05/23/2017 09:29:04 AM	Contoso-ADSrv	jones	CONTOSO	C:\Program data\explorer.exe	C:\Windows\System32\Sysprep	ReadData
05/19/2017 06:25:32 AM	Contoso-HRwks	system	CONTOSO	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\modules\mimikatz	WriteData
05/15/2017 07:46:10 AM	Contoso-mktwks	james	CONTOSO	C:\Program Files\Microsoft Office\root\Office16\winword.exe	C:\Users\%AppData%\Local\Temp\Roaming.exe	DELETE

7 Policy Change

Policy Change		
Audit Policy Change	Enable	Enable
Authentication Policy Change	Enable	Enable
Authorization Policy Change	Enable	Enable
Filtering Platform Policy Change	Disable	Disable
MPSSVC Rule-Level Policy Change	Disable	Disable
Other Policy Change Events	Disable	Enable

8 Privilege Use

Privilege Use		
Non-Sensitive Privilege Use	Enable	Enable
Sensitive Privilege Use	Enable	Enable
Other Privilege Use Events	Enable	Enable

9 System

System		
IPSEC Driver	Disable	Disable
Other System Events	Disable	Disable
Security State Change	Enable	Enable
Security System Extension	Enable	Enable
Security System Integrity	Enable	Enable

10 Global Object Access Auditing

Global Object Access Auditing		
Registry (GOAA)	Optional	Optional
File System (GOAA)	Optional	Optional

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support