



Sign In



Tech Community Live: Microsoft Security

Dec 03 2024, 07:00 AM - 11:30 AM (PST) Microsoft Tech Community

Find out more >

[Home](#) > [Security, Compliance, and Identity](#) > [Core Infrastructure and Security Blog](#)

> WINDOWS 10 CONTROLLED FOLDER ACCESS EVENT SEARCH

[Back to Blog](#)



WINDOWS 10 CONTROLLED FOLDER ACCESS EVENT SEARCH



By



[Tan Tran](#)

Published May 05 2021 05:54 AM

120K Views

[Skip to Primary Navigation](#)



Dear IT Pros,

Ransomware acts with accessing to the files, folders and encrypting them, to respond against it, we need to enable the Windows Defender feature named "Controlled Folder Access" – WDCFA and monitor the Windows Defender Guard Events in Windows Event Viewer. The best way is possibly collecting the related activities by Advanced Hunting features of Microsoft 365 Security or Defender for Endpoint.

Could we search for Event ID by running the advanced hunting query or not?

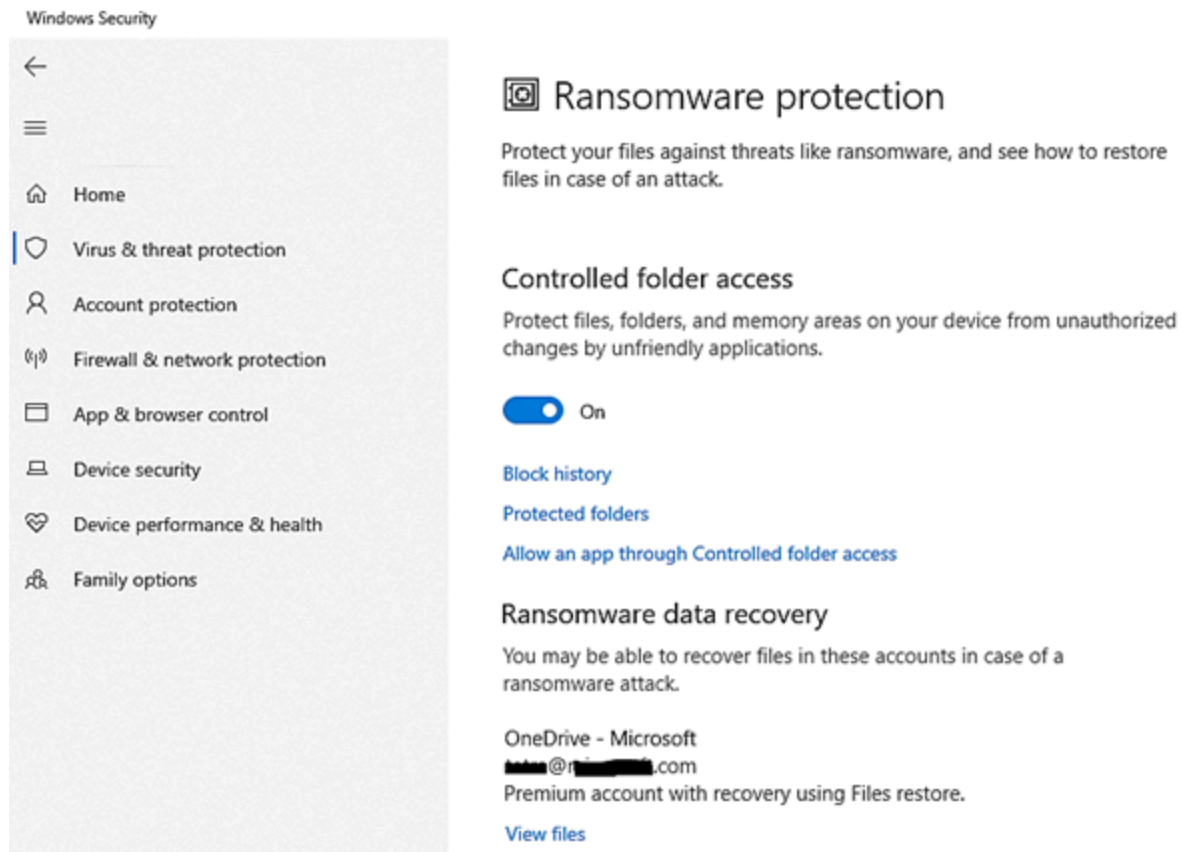
We will discuss the above topic today.

To View or change the list of protected folders

You can use the Windows Security app to view the list of folders that are protected by controlled folder access.

1. On your Windows 10 device, open the Windows Security app.
2. Select **Virus & threat protection**.

3. Under **Ransomware protection**, select **Manage ransomware protection**.



4. If controlled folder access is turned off, you'll need to turn it on. Select **protected folders**.

5. Do one of the following steps:

- To add a folder, select **+ Add a protected folder**.
- To remove a folder, select it, and then select **Remove**.

Note

[Windows system folders](#) are protected by default, and you cannot remove them from the list.

To Enable Controlled Folder Access by powershell command:

> `Set-MpPreference -EnableControlledFolderAccess Enabled`



- If you want to add a file or folder to be protected:

```
PS C:\WINDOWS\system32> Set-MpPreference -ControlledFolderAccessProtectedFolders "C:\Users\...a\OneDrive - Microsoft"
PS C:\WINDOWS\system32> |
```

- To remove a protected folder:

> Remove-MpPreference -ControlledFolderAccessProtectedFolders "C:\Users\abcUser\OneDrive - Microsoft"

```
PS C:\WINDOWS\system32> remove-MpPreference -ControlledFolderAccessProtectedFolders "C:\Users\...a\OneDrive - Microsoft"
PS C:\WINDOWS\system32> Get-MpPreference

AllowNetworkProtectionOnWinServer      : False
AttackSurfaceReductionOnlyExclusions   : {0, 0, 0, 0...}
AttackSurfaceReductionRules_Actions    : {01443614-CD74-433A-B99E-2ECDC078FC25, 26190899-1602-49E8-8B27-EB1D0A1CE869, 3B576869-A4EC-4529-8536-B80A769E899, 5BEB7EFE-FD9A-4556-801D-275E3FFC04CC...}
AttackSurfaceReductionRules_Iids       : {True}
CheckForSignaturesBeforeRunningScan    : True
CloudBlockLevel                         : 0
CloudExtendedTimeout                   : 0
Computer ID                            : 4051E040-OCEA-4733-903F-2729ADE745B6
ControlledFolderAccessAllowedApplications : {C:\Program Files\Microsoft Power BI Desktop\bin\PBIDesktop.exe, C:\Users\...a\AppData\Local\WebEx\WebEx\Applications\ptonecl.exe}
ControlledFolderAccessProtectedFolders : 
DisableArchiveScanning                 : False
DisableAutoExclusions                  : False
DisableBehaviorMonitoring               : False
DisableBlockAtFirstSeen                : False
DisableCatchupFullScan                 : False
DisableCatchupQuickScan                : False
DisableCpuThrottleOnIdleScans          : False
DisableDatagramProcessing               : False
DisableDeferToProcess                  : True
```

- If you want to add a specific app that you trust to access your files and folders, type this command:

> Add-MpPreference -ControlledFolderAccessAllowedApplications "C:\Program Files\Windows Photo Viewer\ImagingDevices.exe"

- If you want to remove a specific app, type this command and indicate its location at the end:

> Remove-MpPreference -ControlledFolderAccessAllowedApplications "C:\Program Files\Windows Photo Viewer\ImagingDevices.exe"

Review controlled folder access events in Windows Event Viewer

The following table shows events related to controlled folder access:

Event ID	Description
5007	Event when settings are changed
1124	Audited controlled folder access event
1123	Blocked controlled folder access event

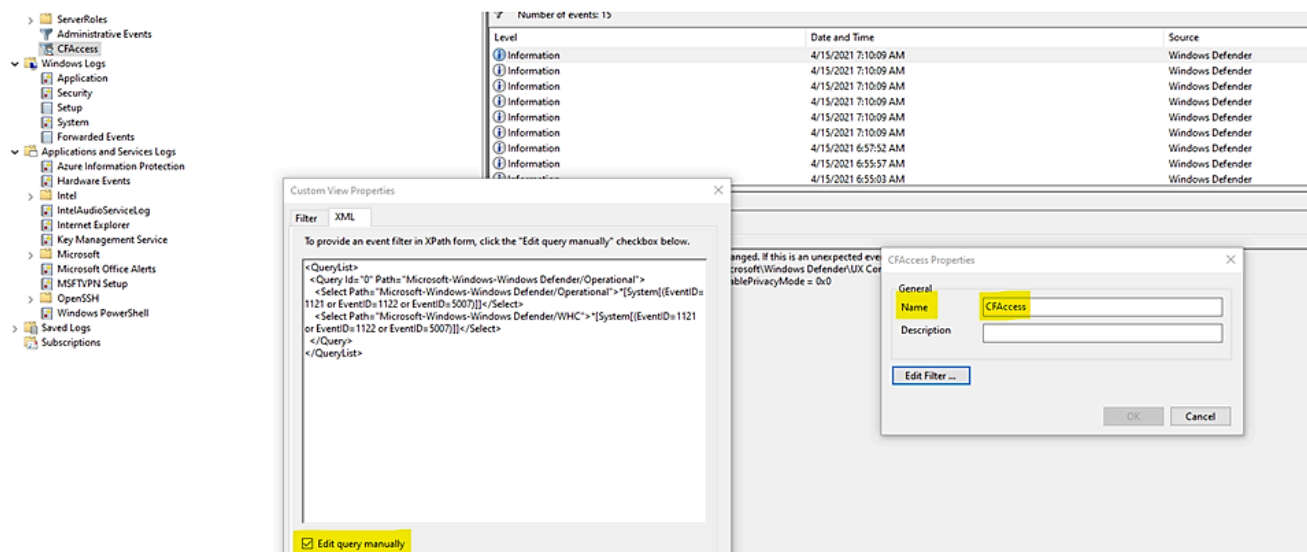
You can review the Windows event log and look for events which were created when controlled folder access of Windows Defender had blocked (or reported in audit mode) an app 's activity of accessing to the related

1. Download the [Evaluation Package](#) and extract the file *cfa-events.xml* to an easily accessible location on the device.

Content of *cfa-events.xml* is shown in the following lines:

```
<QueryList>
  <Query Id="0" Path="Microsoft-Windows-Windows Defender/Operational">
    <Select Path="Microsoft-Windows-Windows Defender/Operational">*[System[(EventID=1121 or EventID=1122 or EventID=5007)]]</Select>
    <Select Path="Microsoft-Windows-Windows Defender/WHC">*[System[(EventID=1121 or EventID=1122 or EventID=5007)]]</Select>
  </Query>
</QueryList>
```

2. Type **Event viewer** in the Start menu to open the Windows Event Viewer.
3. On the left panel, under **Actions**, select **Import custom view....**
4. Navigate to where you extracted *cfa-events.xml* and select it. Alternatively, [copy the XML directly](#).
5. Select **OK**.



Review controlled folder access events in the Microsoft 365 Security.

M365 Security portal, advanced hunting provides detailed information of Windows Defender events as part of its [alert investigation scenarios](#).

You can query Microsoft 365 Security data by using [Advanced hunting](#). For Controlled Folder Access, if you are enable it [audit mode](#), you can use [advanced hunting](#) to see how controlled folder access settings would affect

```
DeviceEvents
| where ActionType in ('ControlledFolderAccessViolationAudited','ControlledFolderAccessViol
```

Advanced Hunting for Controlled Folder Access Events:

Query Table

WDAC- Windows Defender Application Control	DeviceEvents where Timestamp > ago(7d) and ActionType startswith "AppControl" summarize Machines=dcount(DeviceName) by ActionType order by Machines desc
Monthly report on Vulnerability	DeviceTvmSoftwareInventoryVulnerabilities project DeviceName, SoftwareName, Cveld, SoftwareVersion, VulnerabilitySeverityLevel join (DeviceTvmSoftwareVulnerabilitiesKB project AffectedSoftware, VulnerabilityDescription , Cveld , CvssScore , IsExploitAvailable) on Cveld project Cveld , SoftwareName , SoftwareVersion , VulnerabilityDescription , VulnerabilitySeverityLevel, IsExploitAvailable , CvssScore distinct SoftwareName , SoftwareVersion, Cveld, VulnerabilityDescription , VulnerabilitySeverityLevel, IsExploitAvailable

WD-ASR Event	DeviceEvents where ActionType == "AsrOfficeChildProcessAudited" and Timestamp > minTime project BlockedProcess=FileName, ParentProcess=InitiatingProcessFileName, DeviceName, Timestamp
WD-CFA Controlled Folder Access Event	DeviceEvents where ActionType in ('ControlledFolderAccessViolationAudited', 'ControlledFolderAccessViolationBlocked')

- **We could not query by Event ID.**

Until today, the built-in Defender for Endpoint sensor does not allow raw ETW access using Advanced Hunting nor forwards them.

- **In Event Viewer, using XML to filter events related to Windows 10 Defender Guard,**
the Event IDs are listed in the following Event Table:

Feature	Provider/source	Event ID	Description
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	1	ACG audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	2	ACG enforce
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	3	Do not allow child processes audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	4	Do not allow child processes block
	Security-Mitigations (Kernel Mode/User		Block low integrity images

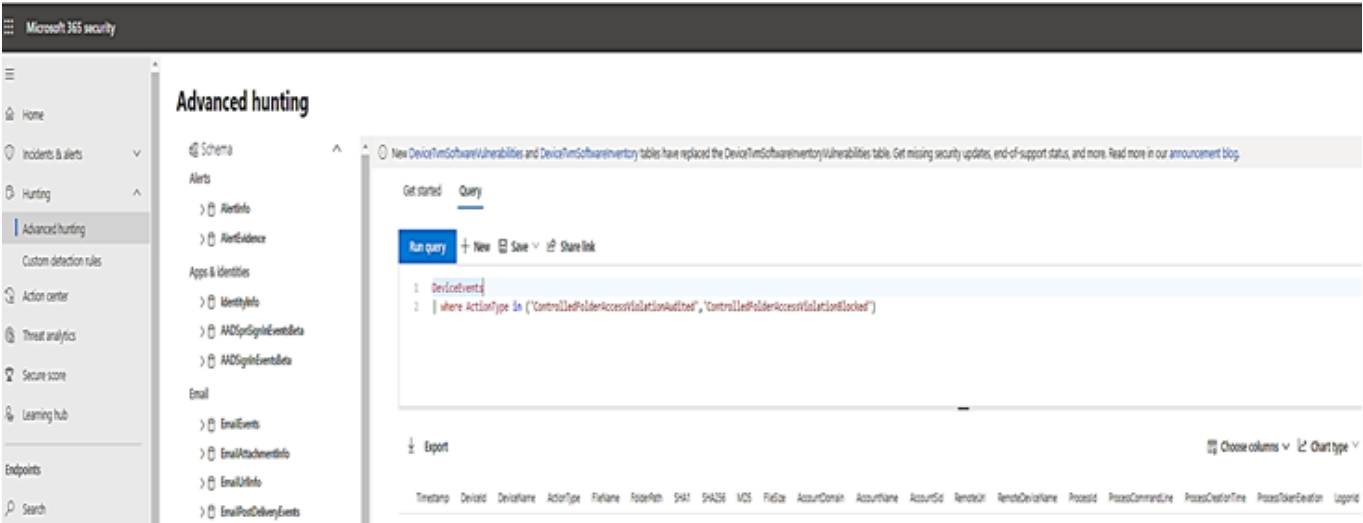
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	6	Block low integrity images block
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	7	Block remote images audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	8	Block remote images block
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	9	Disable win32k system calls audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	10	Disable win32k system calls block
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	11	Code integrity guard audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	12	Code integrity guard block
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	13	EAF audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	14	EAF enforce
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	15	EAF+ audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	16	EAF+ enforce
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	17	IAF audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	18	IAF enforce

[Skip to Primary Navigation](#)

Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	19	ROP StackPivot audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	20	ROP StackPivot enforce
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	21	ROP CallerCheck audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	22	ROP CallerCheck enforce
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	23	ROP SimExec audit
Exploit protection	Security-Mitigations (Kernel Mode/User Mode)	24	ROP SimExec enforce
Exploit protection	WER-Diagnostics	5	CFG Block
Exploit protection	Win32K (Operational)	260	Untrusted Font
Network protection	Windows Defender (Operational)	5007	Event when settings are changed
Network protection	Windows Defender (Operational)	1125	Event when Network protection fires in Audit-mode
Network protection	Windows Defender (Operational)	1126	Event when Network protection fires in Block-mode
Attack surface reduction	Windows Defender (Operational)	5007	Event when settings are changed
Attack surface reduction	Windows Defender (Operational)	1122	Event when rule fires in Audit-mode

Attack surface reduction	Windows Defender (Operational)	1121	Event when rule fires in Block-mode
--------------------------	--------------------------------	------	-------------------------------------

- You could run the queries by using Microsoft 365 Security or Microsoft Defender for Endpoint.



I hope the information is useful, see you next time.

Reference:

- <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o3...>
- <https://www.verboon.info/2019/11/how-to-generate-a-monthly-defender-atp-threat-and-vulnerability-rep...>
- <https://docs.microsoft.com/en-us/power-bi/report-server/configure-scheduled-refresh>
- <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/run-advanced-query-sample-...>
- <https://docs.microsoft.com/en-us/microsoft-365/enterprise/use-windows-powershell-to-create-reports-i...>
- [How to Automate PowerShell Scripts with Task Scheduler \(netwrix.com\)](#)
- <https://docs.microsoft.com/en-us/samples/browse/?products=mdatp>
- <https://github.com/microsoft/MicrosoftDefenderATP-PowerBI>
- <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/api-power-bi?view=o365-wor...>
- <https://docs.microsoft.com/en-us/power-bi/report-server/configure-scheduled-refresh>

1 Comment



You must be a registered user to add a comment. If you've already registered, sign in.
Otherwise, register and sign in.



[Comment](#)

Co-Authors



[TanTran](#)

Version history

Last update: May 05 2021 10:53 AM

Updated by: [TanTran](#)

Labels

TanTran

25

Share



[Skip to Primary Navigation](#)

What's new

- Surface Pro 9
- Surface Laptop 5
- Surface Studio 2+
- Surface Laptop Go 2
- Surface Laptop Studio
- Surface Duo 2
- Microsoft 365
- Windows 11 apps

Business

- Microsoft Cloud
- Microsoft Security
- Dynamics 365
- Microsoft 365
- Microsoft Power Platform
- Microsoft Teams
- Microsoft Industry
- Small Business

Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns
- Order tracking
- Virtual workshops and training
- Microsoft Store Promise
- Flexible Payments

Developer & IT


- Azure
- Developer Center
- Documentation
- Microsoft Learn
- Microsoft Tech Community
- Azure Marketplace
- AppSource
- Visual Studio

Education

- Microsoft in education
- Devices for education
- Microsoft Teams for Education
- Microsoft 365 Education
- Education consultation appointment
- Educator training and development
- Deals for students and parents
- Azure for students

Company

- Careers
- About Microsoft
- Company news
- Privacy at Microsoft
- Investors
- Diversity and inclusion
- Accessibility
- Sustainability

 Your Privacy Choices