LIFARS
your digital world, secured

Defend against Ransomware: Controlled folder access

Defend against Ransomware: Controlled folder access

Ransomware has been a significant and serious threat to organizations. A successful attack not only causes a monetary loss but also inflicts consequential damages due to the loss of information, of assets and, often, of reputation. Although ransomware cannot be completely avoided, there are efficient defenses against this threat that organizations can implement. These defenses include enforcing strict security postures and developing organizational, administrative, and technical controls.

One of such controls which leads to an improved resiliency of an organization against ransomware is a security feature introduced in **Fall Creators Update** (2017). This feature is called "Controlled folder access" and comes as part of Windows Defender Exploit Guard. This feature is available for both Windows 10 and Windows Server 2019.

Controlled Folder access monitors all processes attempting to change data in defined folders: if a process tries to modify files in these protected folders without being authorized to do so, the operation is blocked and an alert is generated. This stops ransomware and prevents malicious programs from making changes, protecting the data and files.

When implementing Controlled folder access, the user or the system administrator may add the necessary applications to a whitelist of applications that are then allowed to access and change the protected folders.

With the default settings, the following folders are protected:

- C:\Users\%username%\Documents
- C:\Users\%username%\Videos
- C:\Users\%username%\Desktop
- C:\Users\%username%\Favorites
- C:\Users\%username%\Music
- C:\Users\%username%\Pictures
- C:\Users\Public\Documents
- C:\Users\Public\Videos
- C:\Users\Public\Desktop
- C:\Users\Public\Pictures

It is not possible to disable the protection of these folders.

Configuration of Controlled Folder Access

Controlled Folder Access can be configured using several different methods:

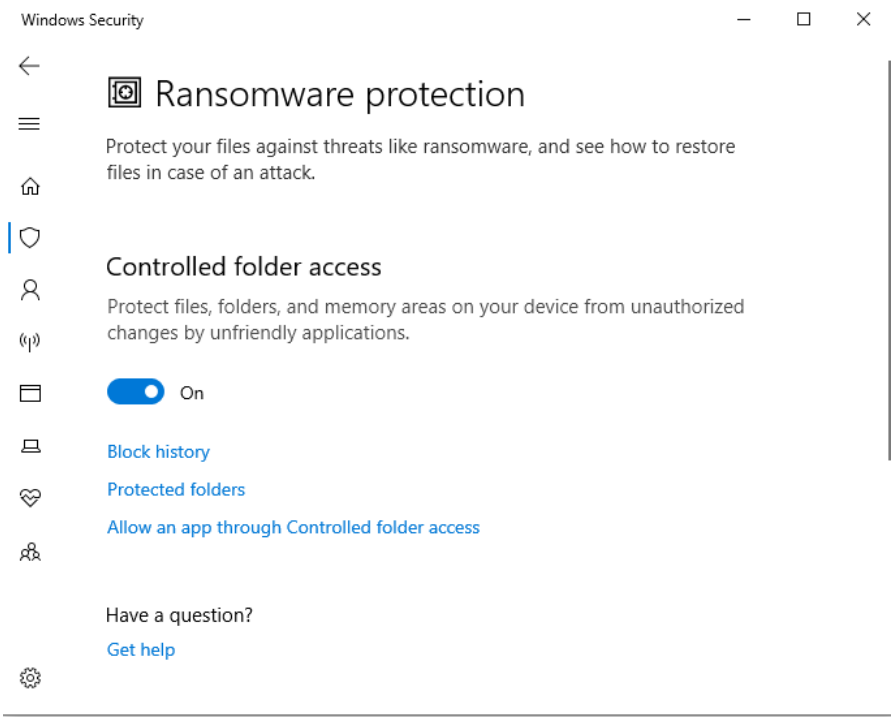
- The Graphic User Interface ("GUI") in Windows Defender Security Center
- PowerShell
- Group policy Object ("GPO")
- Microsoft System Center Configuration Manger ("SCCM")

Below, we show how to configure Controlled Folder Access using the GUI, Powershell and the GPO.

GUI in Windows Defender Security Center

To start the configuration using the GUI, do the following:

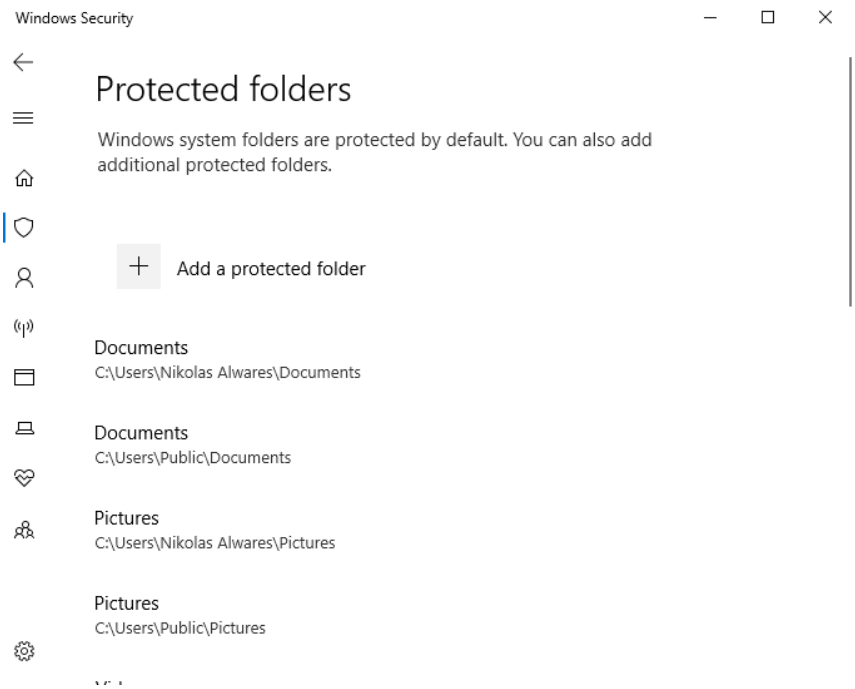
1. Go to the **Start Menu** > **Windows defender security center**
2. Click on **Virus & threat protection**
3. In **Ransomware protection >** click on **Manage ransomware protection**
4. Under the **Controlled folder access >** set the protection to **ON**. A UAC dialog will request you to confirm the system change.



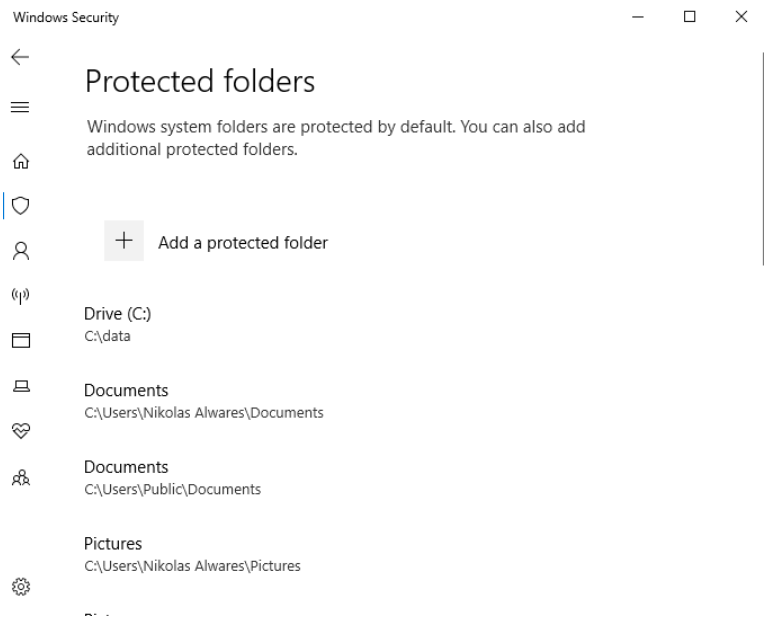
Windows Defender now checks the protected folders and will prevent any modification by unauthorized applications.

If you need to add new folders to the ones Controlled Folder Access already protects, follow the following steps:

1. Go to the **Start Menu** >**Windows defender security center**
2. Go to the **Start Menu** > **Windows defender security center**
3. Click on the **Protected Folder** option in the Windows defender security center

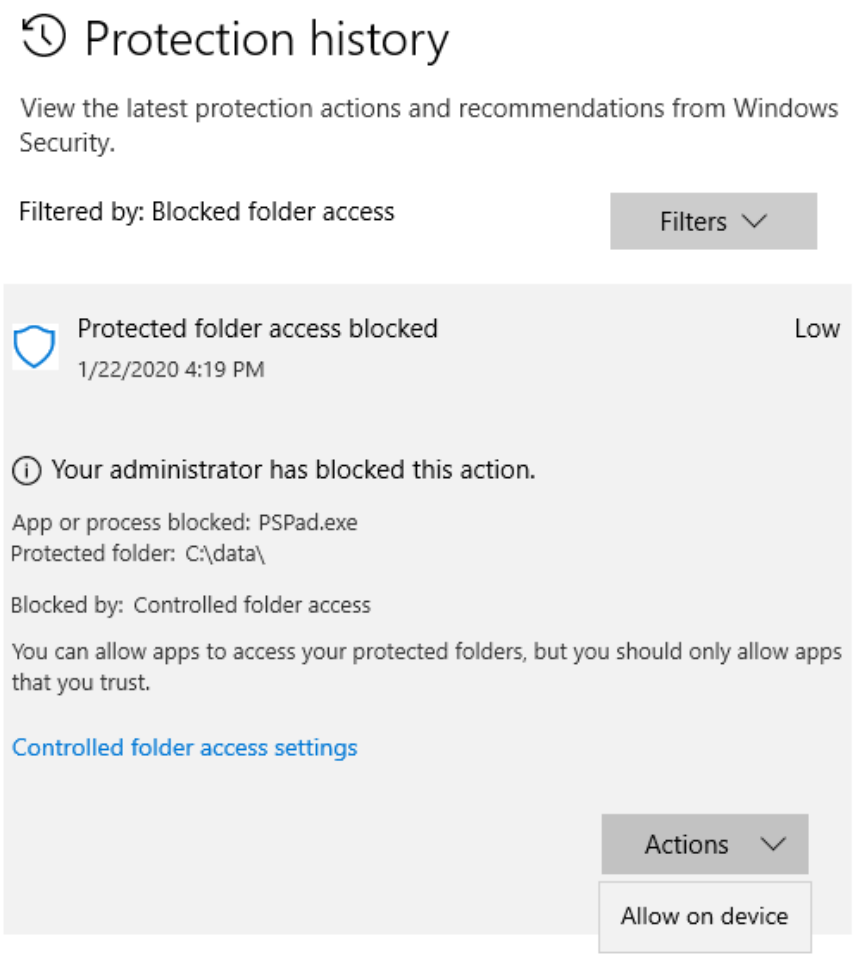


4. Tap on **Add a protected folder**
5. For demonstration purposes, we will add the folder **c:\Data**



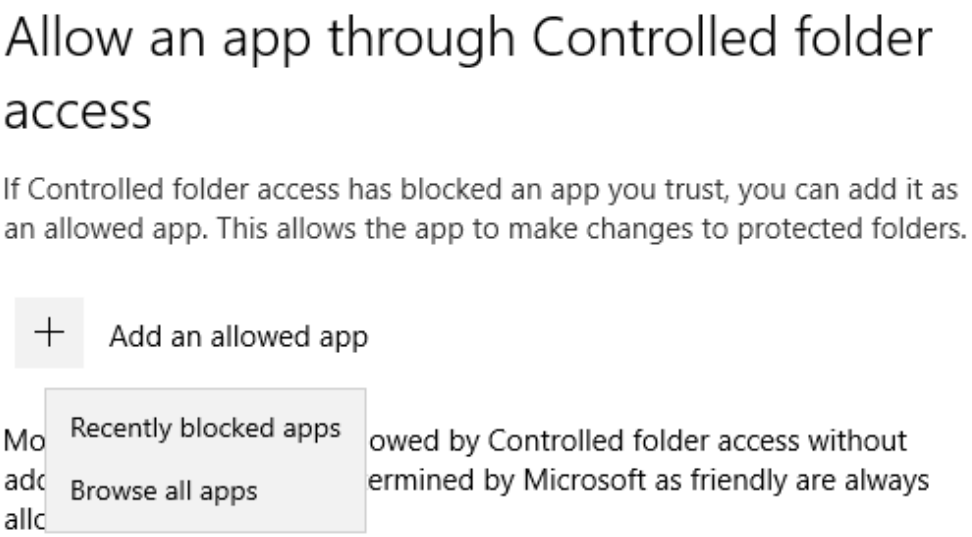
If we try to change the files in this folder using an application that is not authorized, and by default Microsoft applications are trusted, the system generates an alert and blocks the modification.

It is also possible to review the alerts and to whitelist applications in **Protection History**. To enable this, go to **Action** and click on **Allow on device** from the drop down.

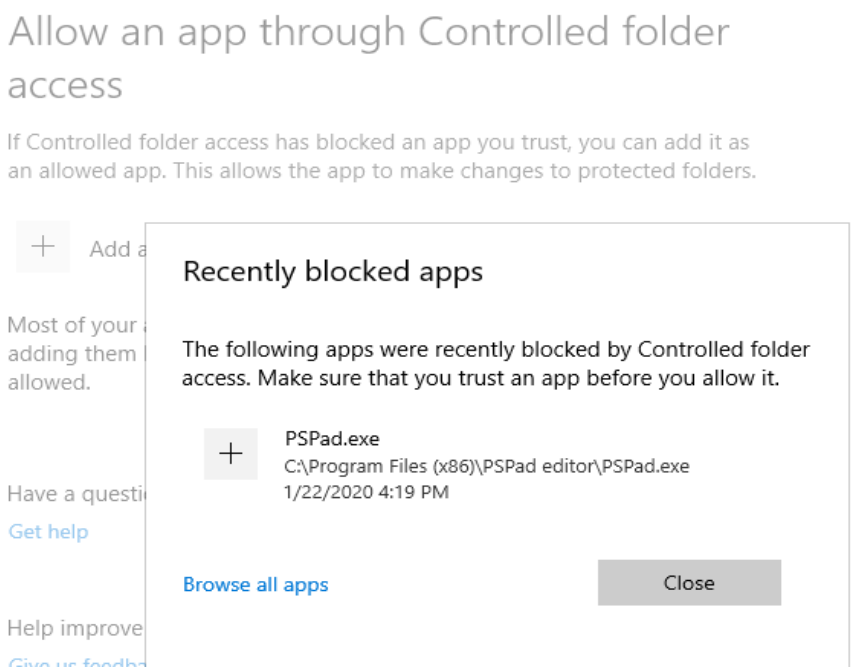


If an application was blocked, adding it to the list of applications authorized to modify data in the protected folder is easy. To do so, follow these steps.

1. Go to the **Start Menu** > **Windows defender security center**
2. Click on **Virus & threat protection**
3. Then click on **Allow an app through Controlled folder access.**
4. To enable the setting, click on **Add an allowed app**.



5. Here we can chose between **Recently blocked** apps (In this case the list of recent apps which was blocked by the Controlled folder access) and **Browse all apps** (In this case a dialog pops up which allows you to select any application on filesystem).



PowerShell

Enabling Controlled folder Access is also possible through PowerShell, as shown in the following steps.

1. Go to the **Start Menu** > Search for **Windows PowerShell**
2. Right click **Windows PowerShell**
3. Click **Run as Administrator**.
4. Use the following command:

```
Set-MpPreference -EnableControlledFolderAccess Enabled
```

If you need to disable Controlled folder access, use this cmdlet:

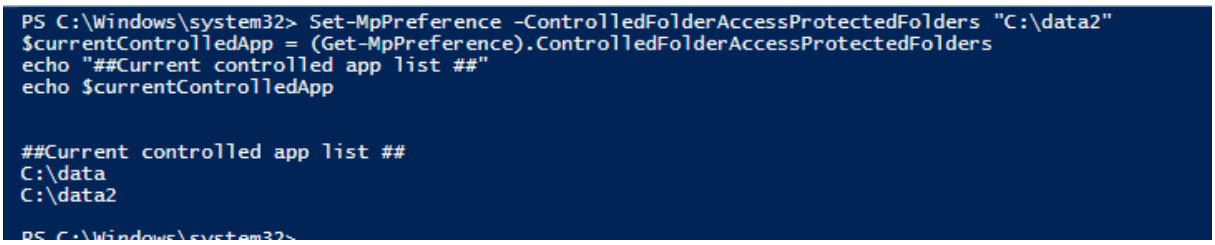
```
Set-MpPreference -EnableControlledFolderAccess Disabled
```

To obtain a list of all non-default protected folders and all whitelisted applications, type:

```
$currentWhiteList = (Get-MpPreference) ControlledFolderAccessAllowedApplications
$currentWhiteList = (Get-MpPreference) ControlledFolderAccessProtectedFolders
echo “##Current controlled app list ##”
echo $currenControlledApp
echo ##Current White List ###
echo $currentWhiteList
```

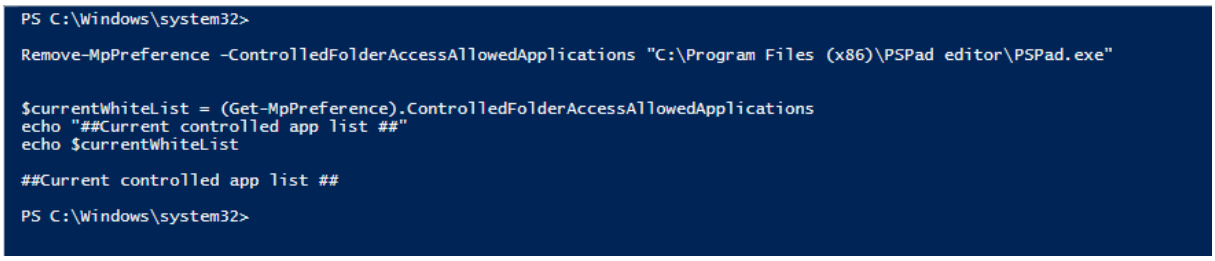
To add a folder to the list of Protected folders, type in the following command:

```
Set-MpPreference -ControlledFolderAccessProtectedFolder “C:\data2”
$currentControlledApp = (Get-MpPreference).ControlledFolderAccessProtectedFolderes
echo “##Current controlled app list ##”
echo $currentControlledApp
```



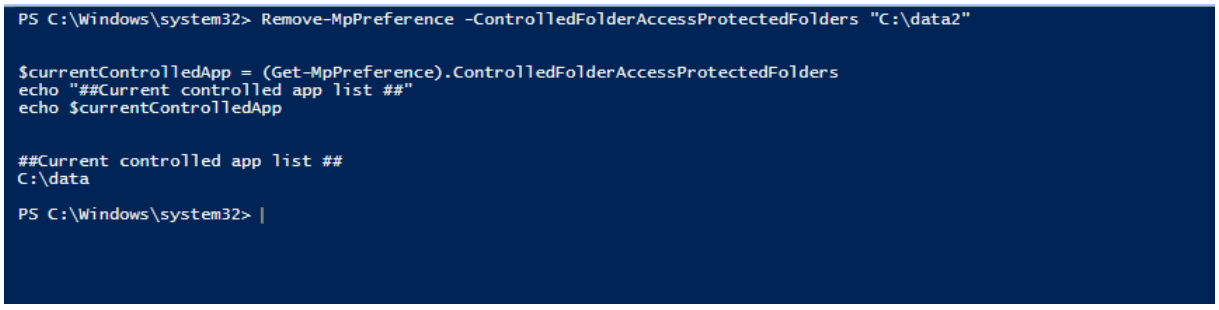
To remove a folder from list of Protected folders, type in the following command:

```
Remove-MpPreference -ControlledFolderAccessProtectedFolders “C:\data2”
```



To remove an application from list of authorized applications, type in the following command:

```
Remove-MpPreference -ControlledFolderAccessAllowedApplications “C:\Program Files (x86)\PSPad editor\PSPad.exe”
```



To obtain a list of alerts from Controlled Folder Access, use the following cmdlet:

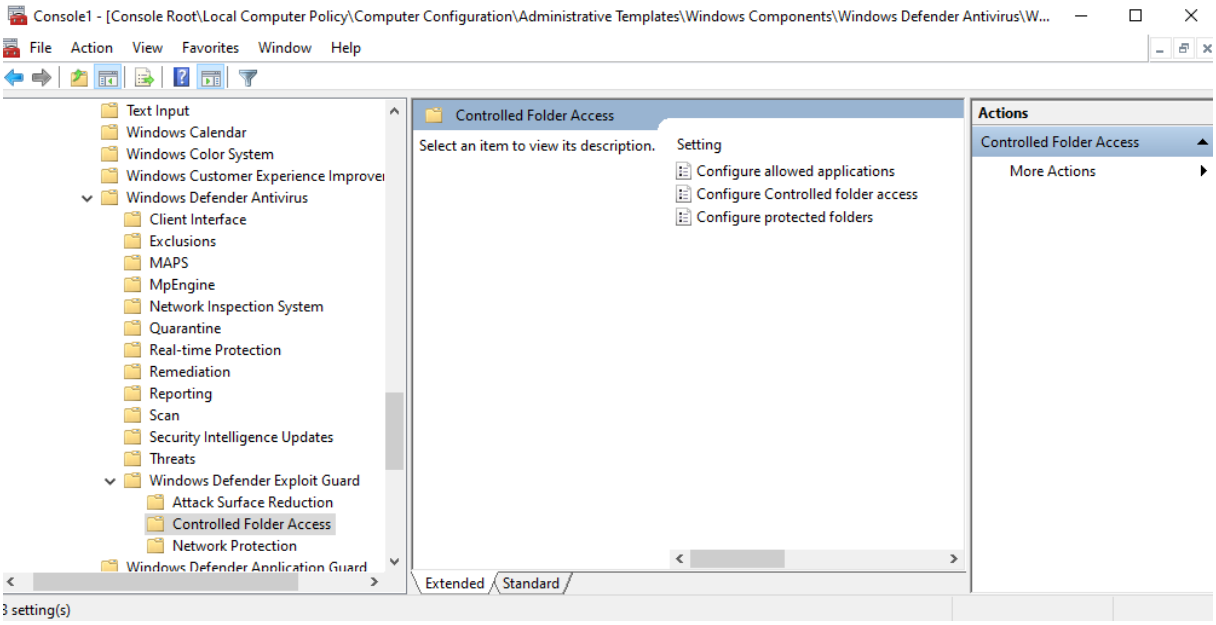
```
$appEvents = Get-WinEvent -LogName “Microsoft-Windows-Windows Defender /Operational”
|

Where-Object {$_.Id -eq “1123”}


ForEach  ($event  in  ($appEvents.toXML()) ) {


echo ([xml]$event).Event.EventData
echo “XXXXXXXXXXXXXXXXXXXXXXXX”

}
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Product Name                    %%827
Product Version                 4.18.1911.3
Unused
ID
Detection Time                  2020-01-19T21:47:19.031Z
User                            DESKTOP-5IPVA59\aeter
Path                            C:\data\Nový priečinok
Process Name                    C:\Program Files\Mozilla Firefox\firefox.exe
Security intelligence Version 1.307.2586.0
Engine Version                  1.1.16600.7
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Configuration using GPO

Controlled Folder Access can also be configured through GPO. To enable Controlled Folder Access, follow the following steps:

1. Go to **Group Policy Management Editor** > **Computer configuration > Administrative templates**
2. Go to **Windows components > Windows Defender Antivirus > Windows Defender Exploit Guard > Controlled folder access**.



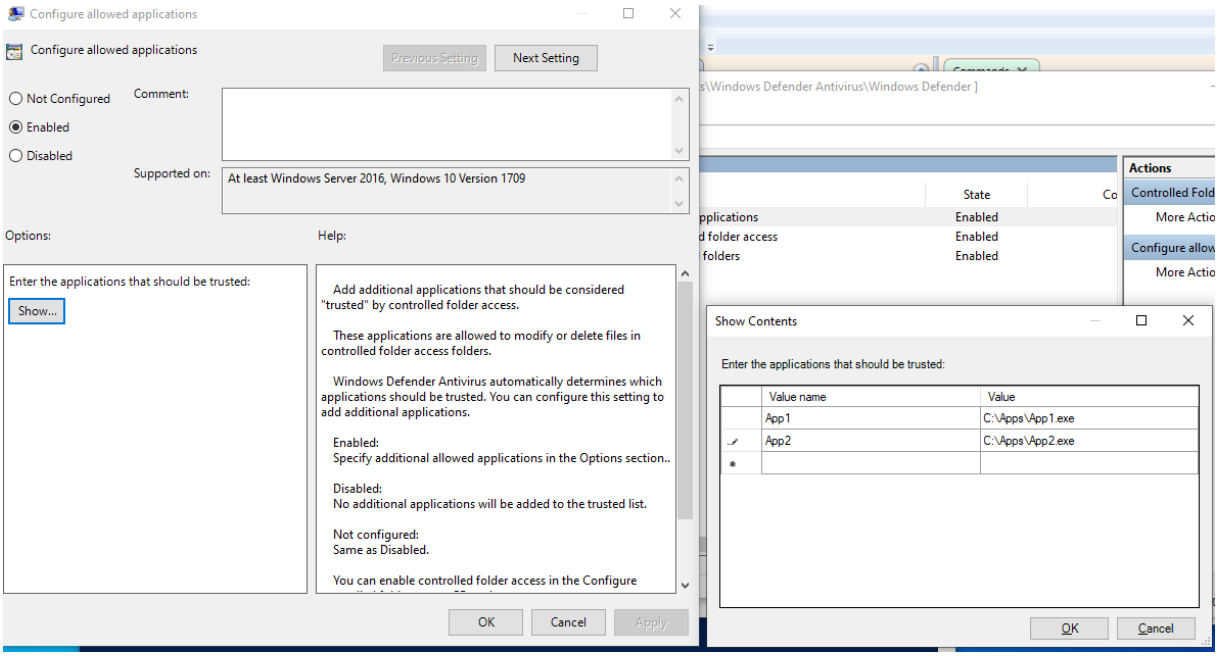
3. Double click the **Configure Controlled Folder Access** setting and set the option to **Enabled**.
4. In the options section you need to specify one of the following:

- **Enable** - Malicious and suspicious (not whitelisted) apps are not allowed to make changes to files in protected folders. A notification is provided in the Windows event log if such an attempt is made.
- **Disable (Default)** - All applications can make changes to files in the protected folders.
- **Audit Mode** – If an application that is not in the whitelist attempts to make a change to a file in a protected folder, the operation is allowed but is also recorded in the Windows event log. This enables you to assess the impact of Controlled folder access in your environment.
- **Block disk modification only**
- **Audit disk modification only**

To add an application to the whitelist

1. From the **Group Policy Management Editor** > go to **Computer configuration >** click **Administrative templates**
2. Go to **Windows components > Windows Defender Antivirus > Windows Defender Exploit Guard > Controlled folder access**.
3. Double-click the **Configure allowed applications** setting
4. Set the option to **Enabled**.

There you can add an application to the whitelist.



To configure protected folders

In the **Group Policy Management Editor** go to **Computer configuration** and click **Administrative templates**

Go to **Windows components > Windows Defender Antivirus > Windows Defender Exploit Guard > Controlled folder access**.

Double-click the **Configure protected folders** setting and set the option to **Enabled**.

Then it is possible to add new folders to the list of folders protected by Controlled Folder Access.

Logging events

To view all events related to Controlled folder access in theWindows Event Logs: **Applications and Services Logs** > **Microsoft** > **Windows** > **Windows Defender** > **Operational (File: c:\Windows\System32\winevt\Logs\ Microsoft-Windows-Windows Defender%4Operational.evtx)**

The table below shows the event ID related to Controlled folder access.

Event ID	Description
5007	**The antimalware platform configuration changed. This setting includes settings for controlled folders access.**
1124	Audited Controlled folder access event
1123	Blocked Controlled folder access event
1127	Blocked Controlled folder access sector write block event
1128	Audited Controlled folder access sector write block event