WINDOWS DEFENDER: ESTABLISH EXCLUSIONS

Security Validation validates the effectiveness of your security technologies. For MSV and MA-SV, this is done by installing Actors in locations around your network. Endpoint security technologies running on the Actor may flag Mandiant services that are required to run Actions. In order for these Actors to be effective and carry out Actions, certain endpoint files pertaining to the execution of these Actors must be added to the allowlist with the security technologies installed on the host.

> The following information is based on the security technology manufacturer's documentation. If the steps do not match your UI, consult the technology's documentation directly.

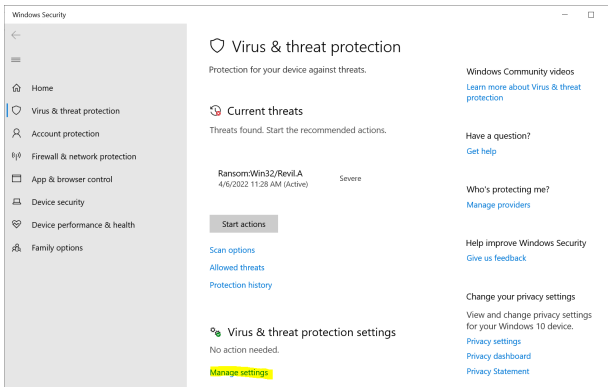
If your network includes Windows Defender, the Mandiant Advantage team recommends creating exclusions within Windows Defender. These exclusions quiet detections for known paths and allow trusted processes to run. There are four different methods that you can use:

- Local UI
- PowerShell (administrator)
- Registry
- Domain Level GPO Exclusions

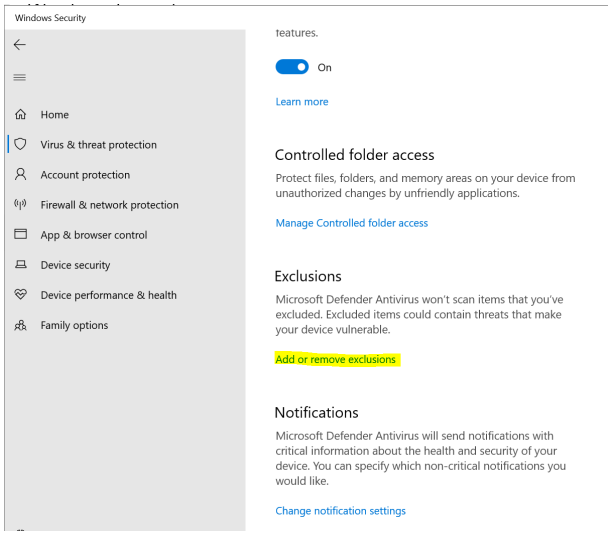
> If your security controls prevent you from using wildcards, you can use the full filenames or hashes instead. If you choose to use the hashes, Windows Defender needs to be updated for each Security Validation release. A list of the filenames and their hashes (for the current version) is located in **Windows 64-bit Actor Artifacts and Services (https://docs.mandiant.com/home/msv-windows-64-bit-actor-artifacts-and-services)**.

Local UI

1. Navigate to **Start** > **Settings** > **Updates and Security** > **Windows Security** > **Virus & threat protection** and select **Manage Settings**.



2. Scroll down to the Exclusions section and select **Add or remove exclusions**.

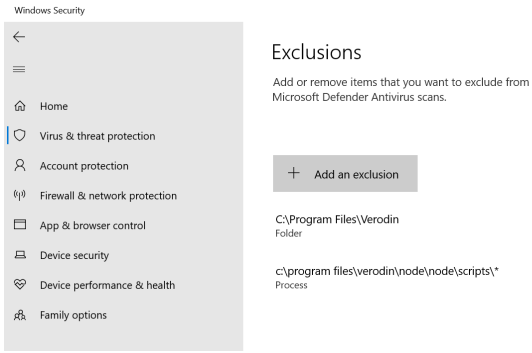


3. Select **Add an exclusion** and add both of the following:

   Folder: `C:\Program Files\Verodin`

   Process: `C:\Program Files\Verodin\node\node\scripts\*`

   RDV should be able to execute after these exclusions are in place.



PowerShell (administrator)

As an administrator, you can add the required exclusions through PowerShell:

```
Add-MpPreference -ExclusionPath "C:\Program Files\Verodin\" -Force
```

```
Add-MpPreference -ExclusionProcess "C:\Program Files\Verodin\node\node\scripts\*"
```

Registry

You can find the exclusions in the registry here: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions`.

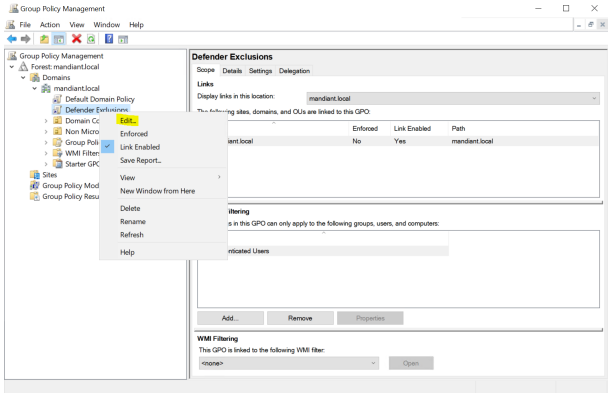
In this registry entry, you see *Paths* and *Processes*. You can add them there manually or run the following:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths]
"C:\\Program Files\\Verodin\\"=dword:00000000
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes]
"C:\\Program Files\\Verodin\\node\\node\\scripts\\*"=dword:00000000
```

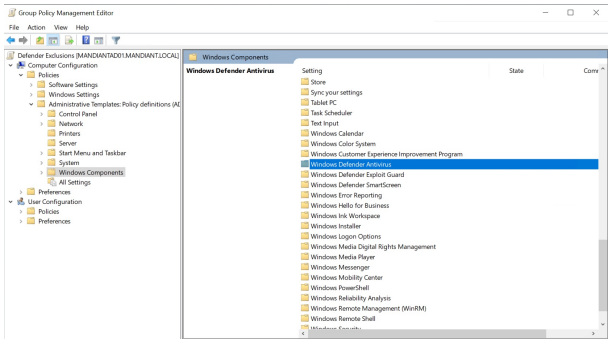
Domain Level GPO Exclusions

If Windows Defender is being used and it's managed by GPO, here's a quick overview on how to add those exclusions. These exclusions must be added at the Domain level and the user must have permissions to edit GPOs.

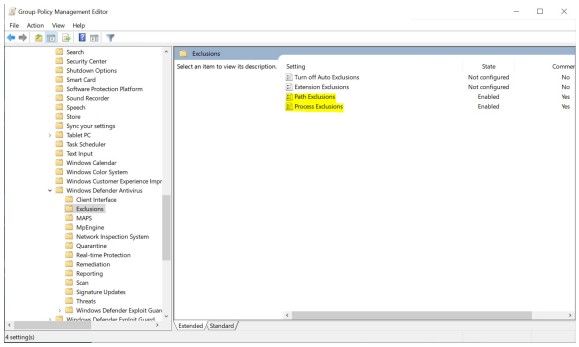
1. **Start** > **Run** > **gpmc.msc** (you must have permissions to modify GPOs). If Group Policy is not installed, you can download the remote tools pack which contains these items.
2. Go to **Forest** > **Domains** > **Domain Name** and either edit an existing policy or create a new one.

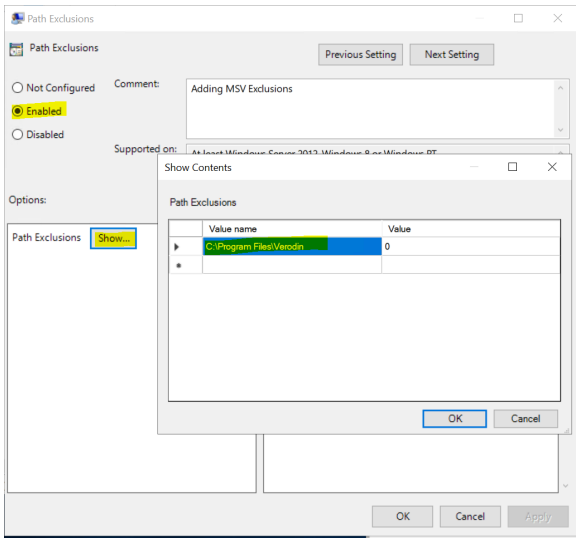


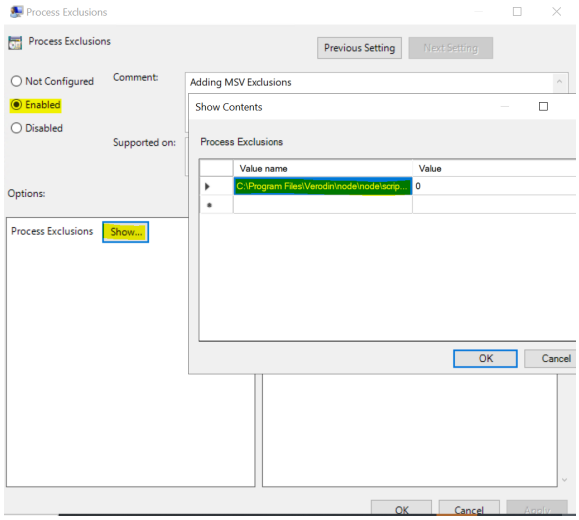
3. Select **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Windows Defender Antivirus** > **Exclusions**.



4. Edit the **Path Exclusions** and **Process Exclusions** to include the MSV folder and processes.
    a. For Path: `C:\Program Files\Verodin`
    b. For Process: `C:\Program Files\Verodin\node\node\scripts\*`







5. Make sure the group policy is applied to the correct systems and you should see the exclusions locally.