How to configure VirusScope in a profile

Click ‘Configuration Templates’ > ‘Profiles’ > click the name of a Windows profile > 'Add Profile Section' > 'VirusScope'

- 'VirusScope' is a CCS feature which monitors the activity of running processes and generates alerts if they take threatening actions.
- The feature uses a system of 'recognizers' to detect malicious behavior and thus identify brand-new malware.
- You can set VirusScope to take one of the following actions if it finds a threat:
    - Generate an alert. The user can decide whether to allow or block the process.

      OR

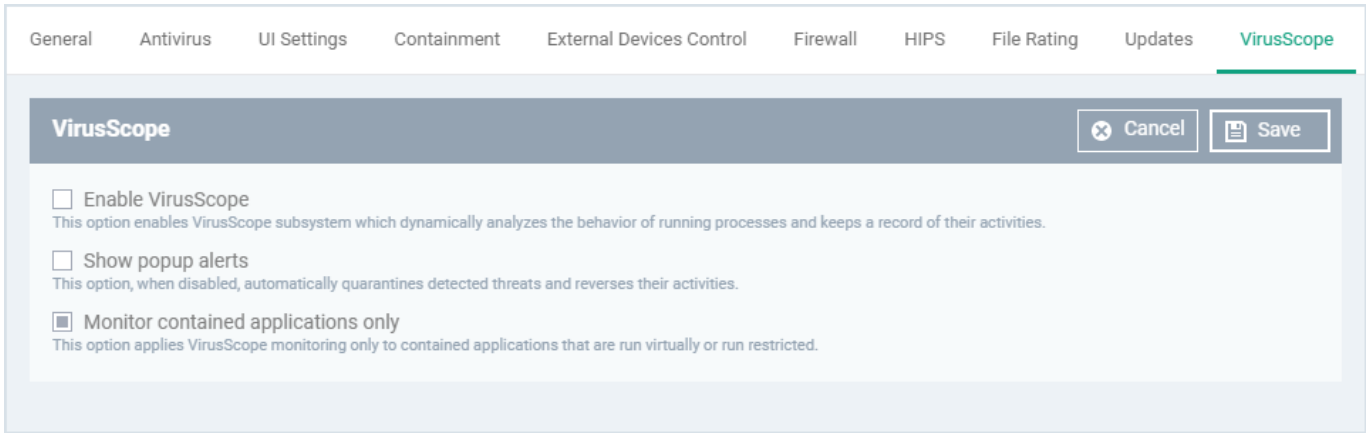
    - Automatically quarantine the process and reverse any actions that it took.
- This article explains how to configure VirusScope in a Windows profile

Configure VirusScope

- Login to Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'
- Click the ‘Profiles’ tab
- Open the Windows profile applied to your target devices
    - Open the 'VirusScope' tab if it has already been added to the profile

      OR

    - Click 'Add Profile Section' > 'VirusScope' if it hasn't yet been added



- **Enable VirusScope** - Activate or deactivate VirusScope. If enabled, VirusScope monitors the activities of all running processes. When it detects suspicious activity, it can show an alert or automatically quarantine the threat. You can choose which one in the 'Show pop-up alerts' setting.

- **Show popup alerts** - Configure whether or not alerts are shown to end-users when VirusScope detects suspicious activity.

    - **Enabled** - VirusScope shows an alert on the endpoint when it finds a threat. The user can block or ignore the threat.

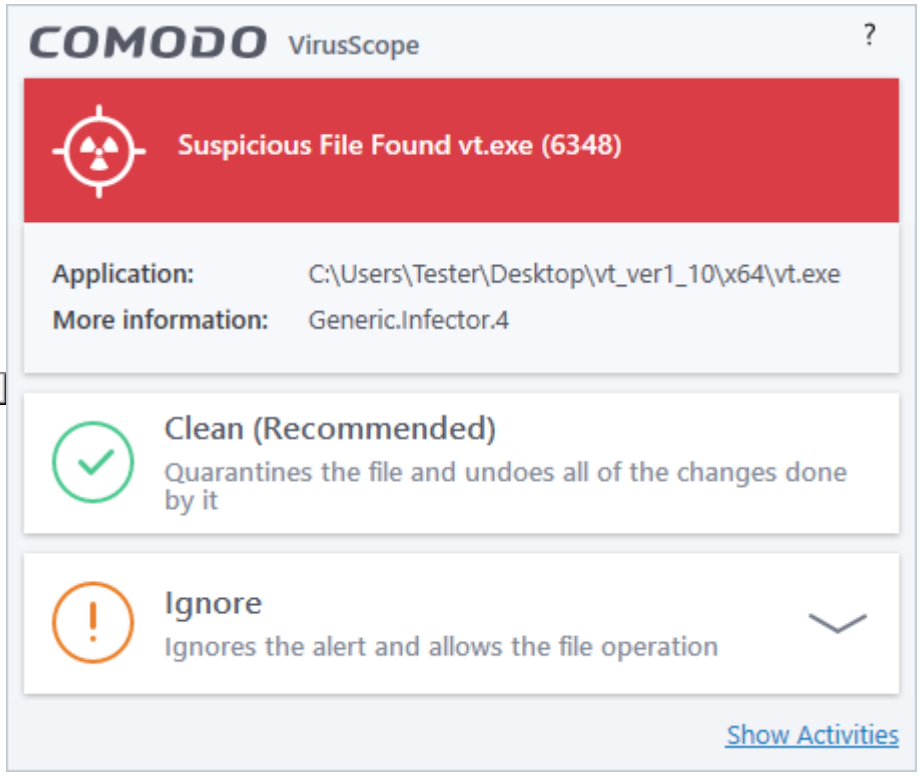
    - **Disabled** - No alert is shown on the endpoint. VirusScope quarantines the threat and reverses its activities.

- **Monitor contained applications only** - Choose whether VirusScope should track every process on the host, or only processes which are running in the container. See this wiki if you want to learn more about the container.

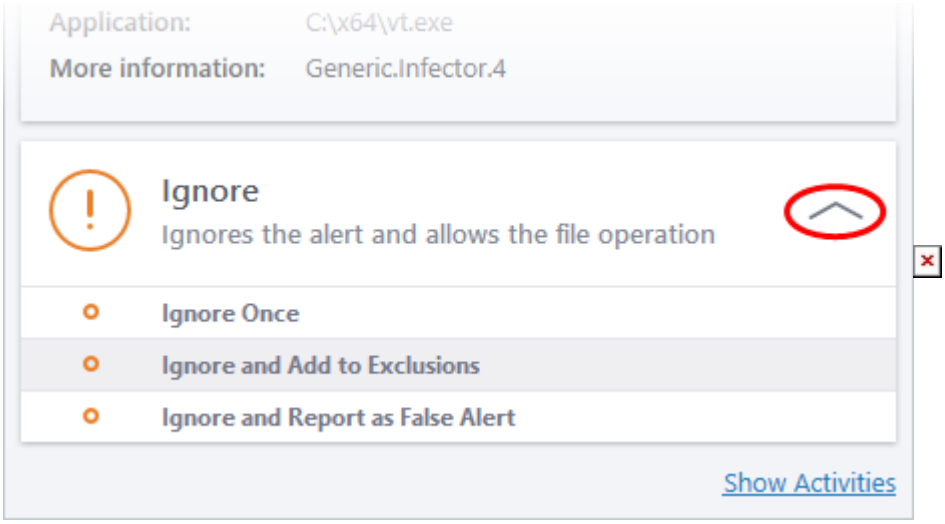
- Click 'Save'.

VirusScope Alerts

If 'Show Popup Alerts' is enabled, end-users will see a notification each time VirusScope discovers a potential threat:

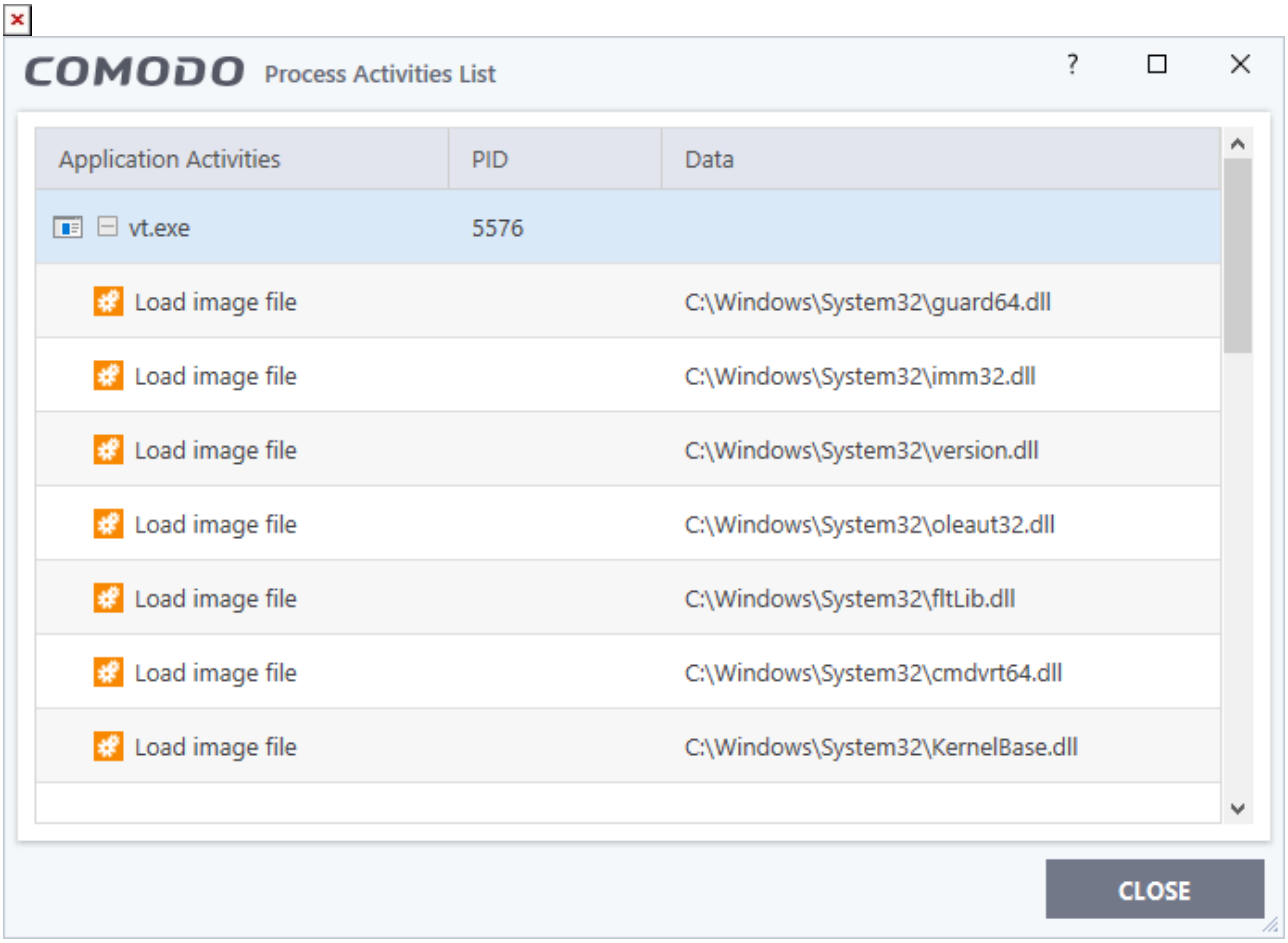


- **Clean –** Kills the process, moves the parent application to quarantine, and reverses any changes made by the process.
- **Ignore –** Allows the process to continue running. Users must then choose one of the following options:



  - **Ignore Once -** The process is allowed to run this time only. Another alert is shown if the process attempts to run again.
  - **Ignore and Add to Exclusions -** The file is allowed to run and will not be flagged as a threat in the future.
  - **Ignore and Report as False Alert –** The file is allowed to run and CCS submits the file to Xcitium for analysis. If the false-positive is verified (and the file is trustworthy), it will be added to the Xcitium safe list.

- **Show activities –** Opens a list of actions that the process performed during its runtime:



- **PID -** The process identification number.
- **Data -** The file affected by the action.
- **Activity legend:**
  - **- File action:** The process performed a file-system operation (create/modify/rename/delete file)
  - **- Registry:** The process performed a registry operation (create/modify a registry key)
  - **- Process:** The process spawned a child process.
  - **- Network:** The process attempted to establish a network connection.

Further Reading:

How to configure containment in a Windows profile

How to manage programs running in containment on your endpoints