How to configure antivirus scan settings in CCS for Linux

Click 'Antivirus' > 'Scanner Settings'

- CCS leverages multiple technologies, including real-time monitoring and on-demand scans, to keep endpoints totally free of malware
- You can set up the behavior of the antivirus scanner for different types of scans
- You can also exclude files, folders and processes that should be skipped by the scans
- The antivirus settings
    - Real time scanning
    - Manual scanning
    - Scheduled scanning
    - Exclusions

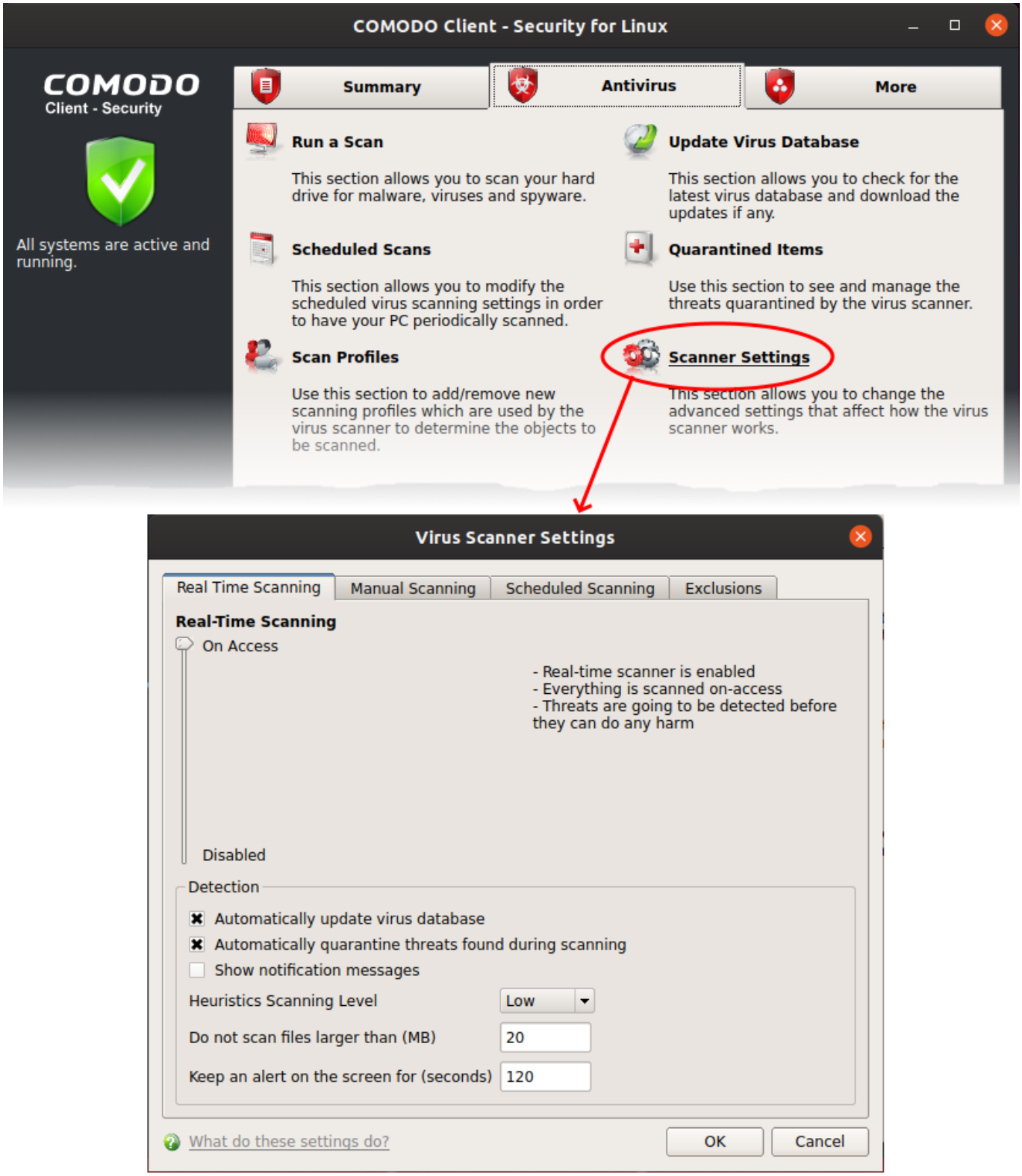
The antivirus settings

Click 'Antivirus' > 'Scanner Settings'

- The settings area lets you configure real-time scans, manual scans, scheduled scans and exclusions.
- The settings you implement here will apply to all future scans of that type.
- Items added to 'Exclusions' are omitted from all types of scan

Open scanner settings

- Open xcitium Client Security
- Click the 'Antivirus' tab
- Click 'Scanner Settings'



The virus scanner settings interface has the following tabs:

- Real Time Scanning - Configure the 'always-on' virus monitor
- Manual Scanning - Configure scanner behavior for on-demand scans
- Scheduled Scanning - Configure scanner behavior for automated-scheduled scans
- Exclusions - View and manage items skipped by virus scans.

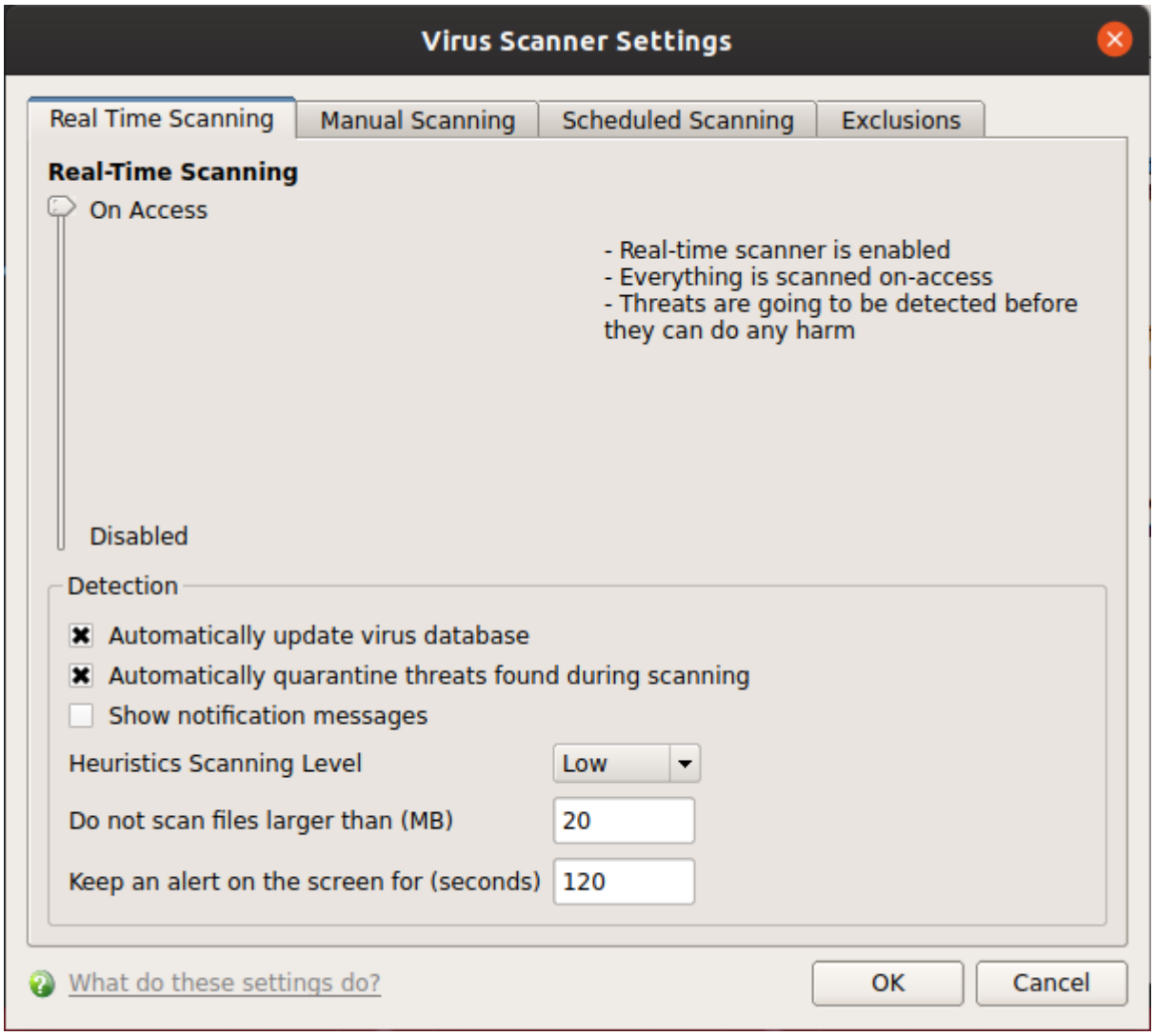
Real Time Scan Settings

Click 'Antivirus' > 'Scanner Settings' > 'Real Time Scanning'

- The real-time scanner is the 'always on' virus monitor which runs in the background, checking files when they are opened, copied or downloaded.
- The real-time scanning area lets you enable or disable the scanner and configure scan options. We highly recommend you keep the real-time scanner active at all times.

Configure real time scanner settings

- Click 'Antivirus' > 'Scanner Settings'
- Click the 'Real Time Scanning' tab, if it is not already open



Real-Time Scanning

- Use the slider to activate or deactivate the real-time virus monitor:
  - On Access - Any file opened is scanned before it is allowed to run.
  - Disabled - Switches the real-time scanner off.

Please note: Real-time scanning is not supported on Debian. This feature is not available on Debian.

Detection Settings

- **Automatically update virus database** - CCS checks for and downloads the latest database at system start-up and regular intervals thereafter (Default = Enabled).

- **Automatically quarantine threats found during scanning** – Select whether or not CCS should automatically take action against malware found by the scan (Default = Disabled).
    - **Enabled** = CCS moves detected malware into an encrypted holding area known as 'quarantine'. Files in quarantine cannot run and pose no threat to your system.

      Click 'Antivirus' > 'Quarantined Items' to review quarantined files. You can restore items to their original location or permanently delete them. See this wiki to read more.

    - ??**Disabled** = CCS shows an alert when a malware is found, with its details. You can choose to clean the malware or to ignore the alert.

- **Show notification messages** - Alerts appear at the bottom-right of the screen whenever malware is found and moved to quarantine. Available only if 'Automatically quarantine threats found during scanning' is enabled. (Default = Disabled).

- **Heuristics Scanning Level** - Heuristics is a technology that analyzes a file to see if it contains code typical of a virus. It is about detecting 'virus-like' attributes rather than looking for a signature which exactly matches a signature on the blacklist. This allows CCS to detect brand new viruses even that are not in the current virus database.

  The drop-down menu lets you select a sensitivity level. The sensitivity level determines how likely it is that heuristics will decide a file is malware:

    - **Off** - Disable heuristic scanning. This means that virus scans only use the 'traditional' virus database to determine whether or not a file is malicious.

    - **Low** - Least likely to decide that an unknown file is malware. Generates the fewest alerts. Despite the name, this setting combines a very high level of protection with a low rate of false positives. xcitium recommends this setting for most users. (Default)

    - **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.

    - **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives.

- **Do not scan files larger than** - Specify the largest file size that the antivirus should scan. CCS will not scan files bigger than the size specified here (Default = 20 MB).

- **Keep an alert on the screen for** - Specify the length of time that virus alerts should stay on the screen. (Default = 120 seconds).

Click 'OK' to apply your changes.

Manual Scanning

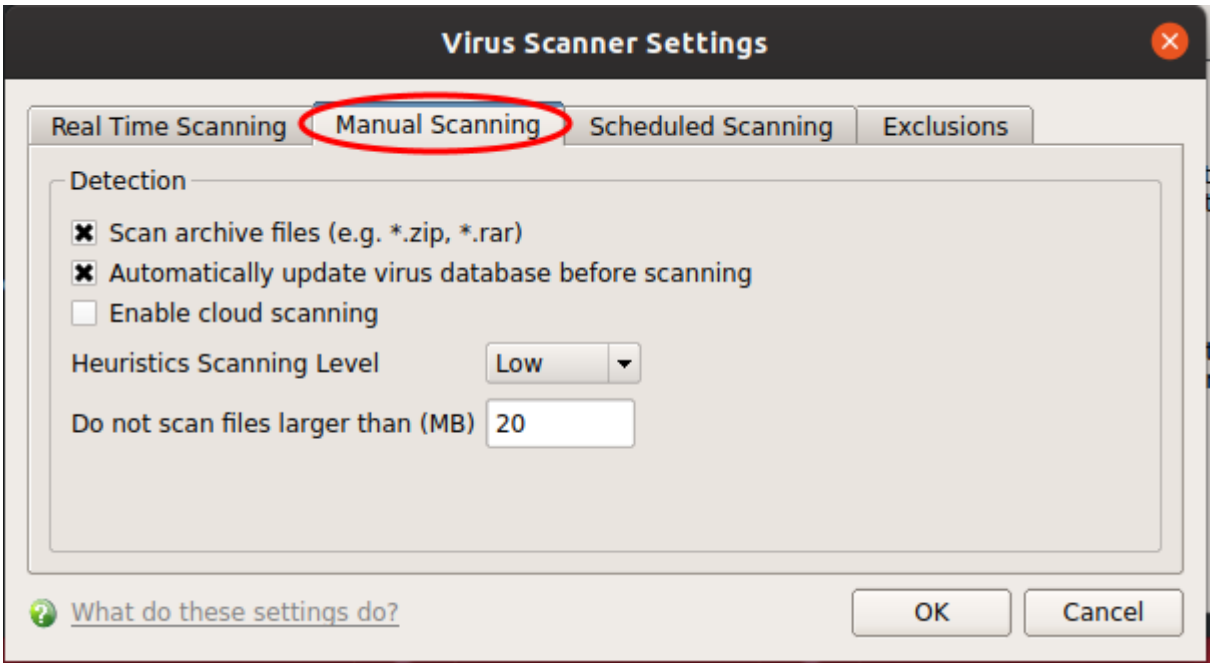
Click 'Antivirus' > 'Scanner Settings' > 'Manual Scanning'

The options you set here apply to all on-demand scans on your computer. For example, these settings are used when:

- You click 'Scan Now' on the home screen then run a full or quick scan
- You scan an item by dragging it into the scan-box on the home screen
- You scan a file in the 'Run A Scan' from the 'Antivirus' menu

Configure manual scan settings

- Open xcitium Client Security
- Click 'Antivirus' > 'Scanner Settings'
- Click the 'Manual Scanning ' tab



Scan archive files - The scan will include compressed file formats such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives (Default = Enabled).

Automatically update virus database before scanning - Check for and download the latest virus signature database prior to running a scan (Default = Enabled).

Enable cloud scanning - Improves scan accuracy by augmenting the local scan with an online look-up of xcitium's latest virus database. Cloud Scanning means CCS can detect the latest malware even if your database is out-dated. (Default = Disabled).

Heuristics Scanning Level - See the description above.

Do not scan files larger than - See the description above.

- Click 'OK' to apply your changes.

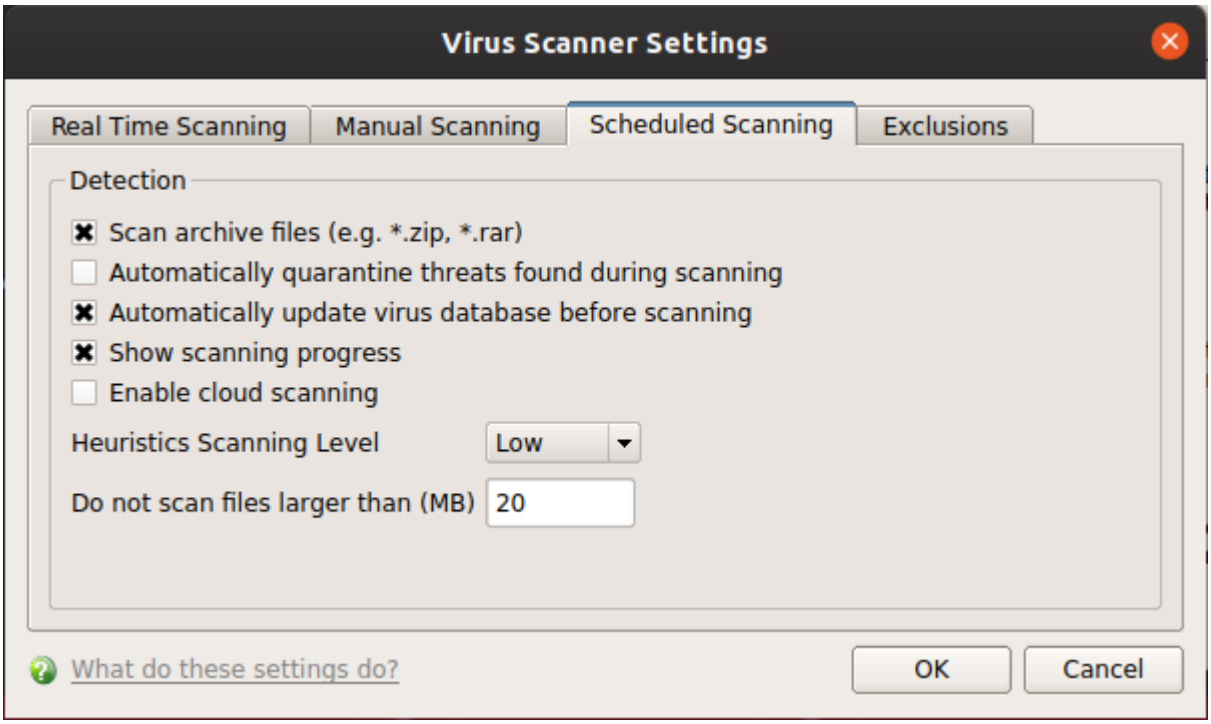
Scheduled Scanning

Click 'Antivirus' > 'Scanner Settings' > 'Scheduled Scanning':

- The options you set in the 'Scheduled Scanning' tab apply to all your scheduled scans. See this wiki for help to create scan schedules.

Configure scheduled scan settings

- Open xcitium Client Security
- Click 'Antivirus' > 'Scanner Settings'
- Click the 'Scheduled Scanning ' tab:



The options in this pane are similar to those for manual scanning settings, except for:

Automatically quarantine threats found during scanning - See the description in the 'real-time scanner settings' section

Show scanning progress - Displays a progress bar when a scheduled scan starts. Clear this box if you do not want to see the scan progress status **(Default = Enabled)**.

- Click 'OK' to apply your changes.

Exclusions

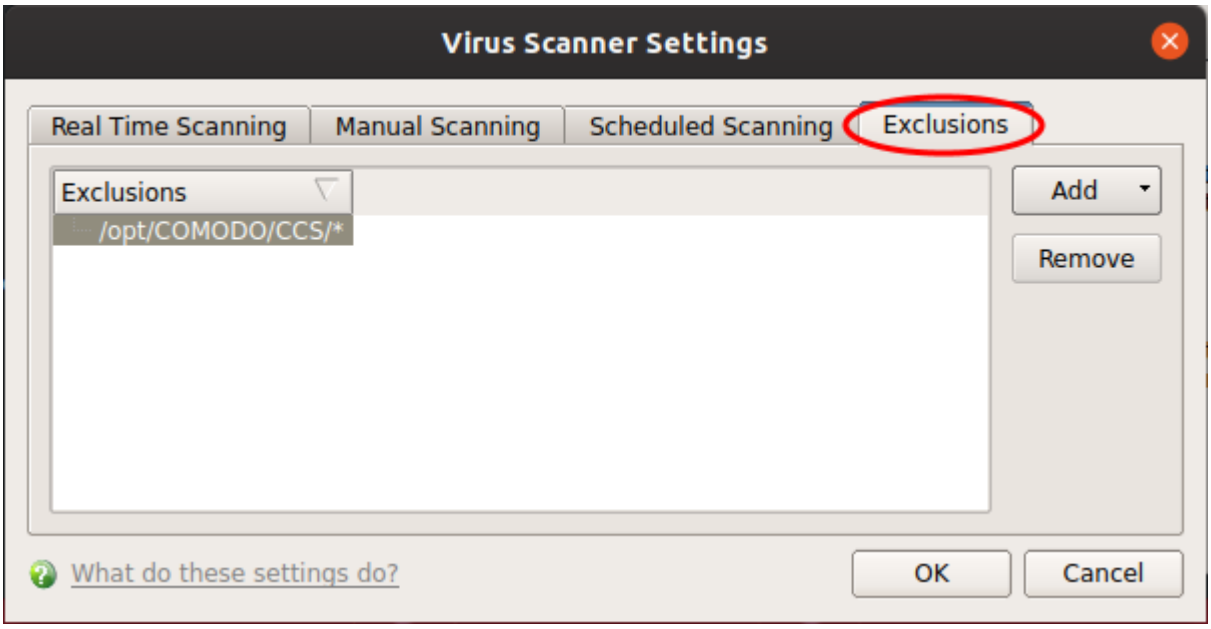
Click 'Antivirus' > 'Scanner Settings' > 'Exclusions'.

- The exclusions area shows files and paths that you have chosen to skip during virus scans.

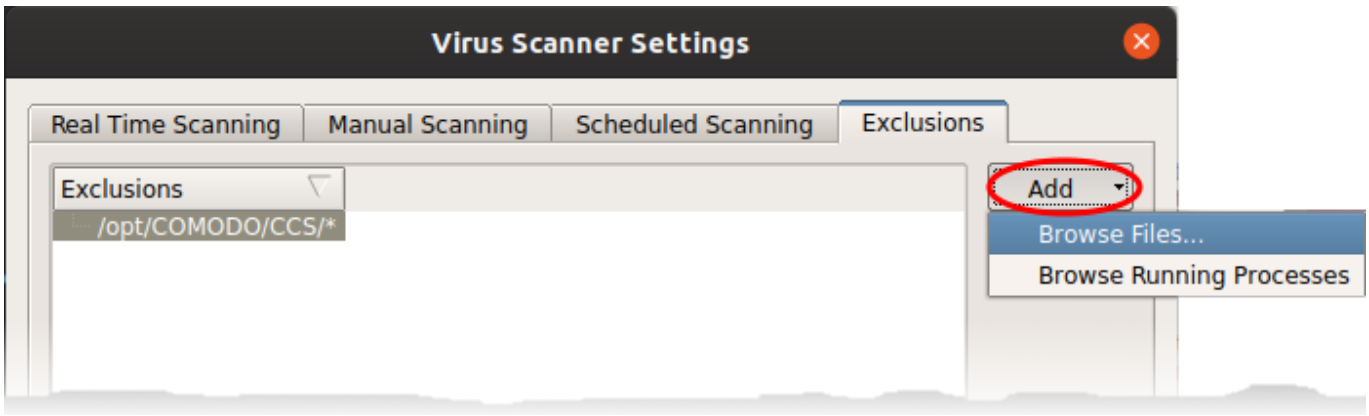
- CCS will not generate an alert for an excluded item, even if the item is rated as malicious in the global blacklist.
- Items may have been added to this list because you selected 'Ignore' at the scan results window, or because you added them to exclusions at an alert.
- Use this interface to add or remove exceptions.

Add and manage exclusions

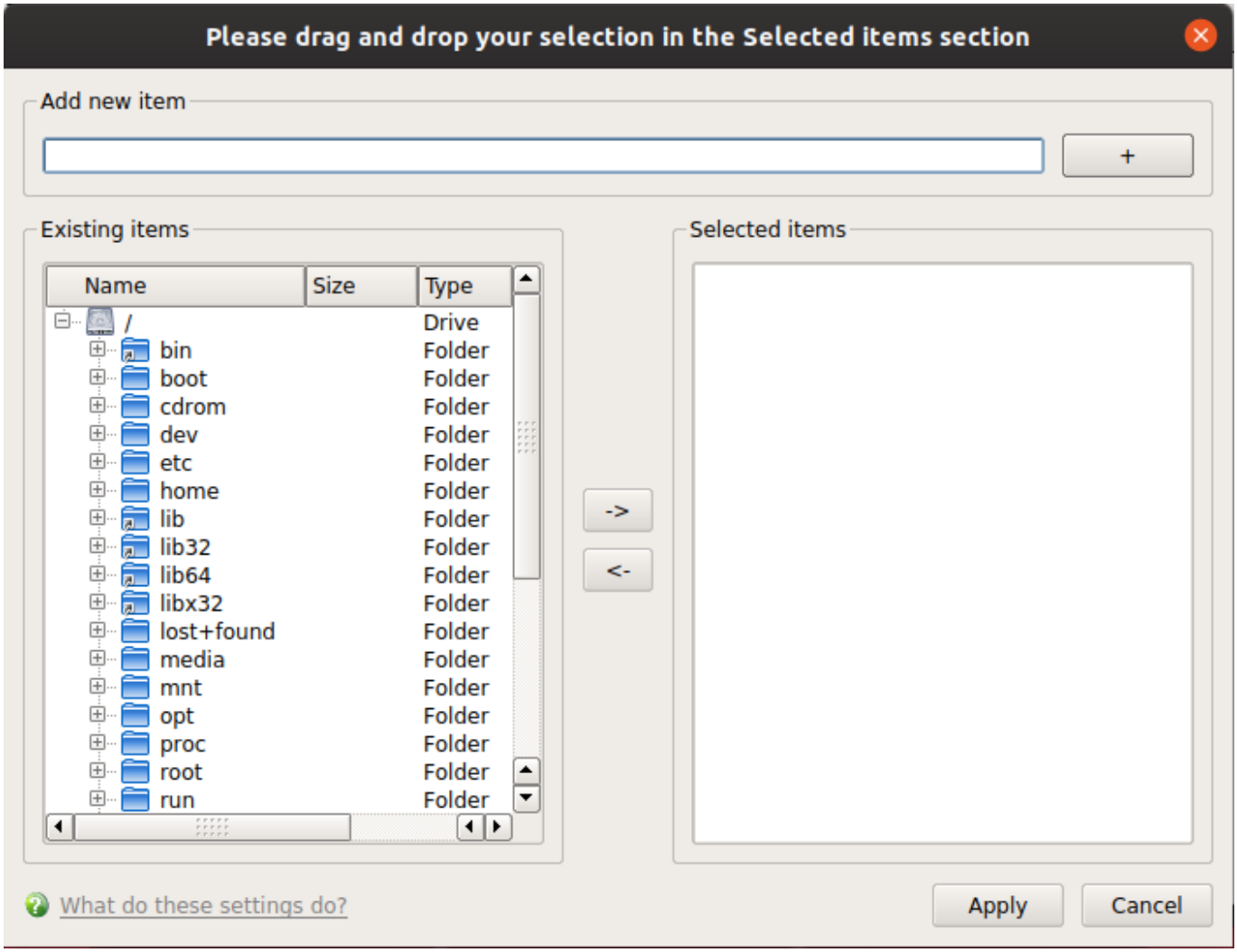
- Open xcitium Client Security
- Click 'Antivirus' > 'Scanner Settings'
- Click the 'Exclusions' tab:



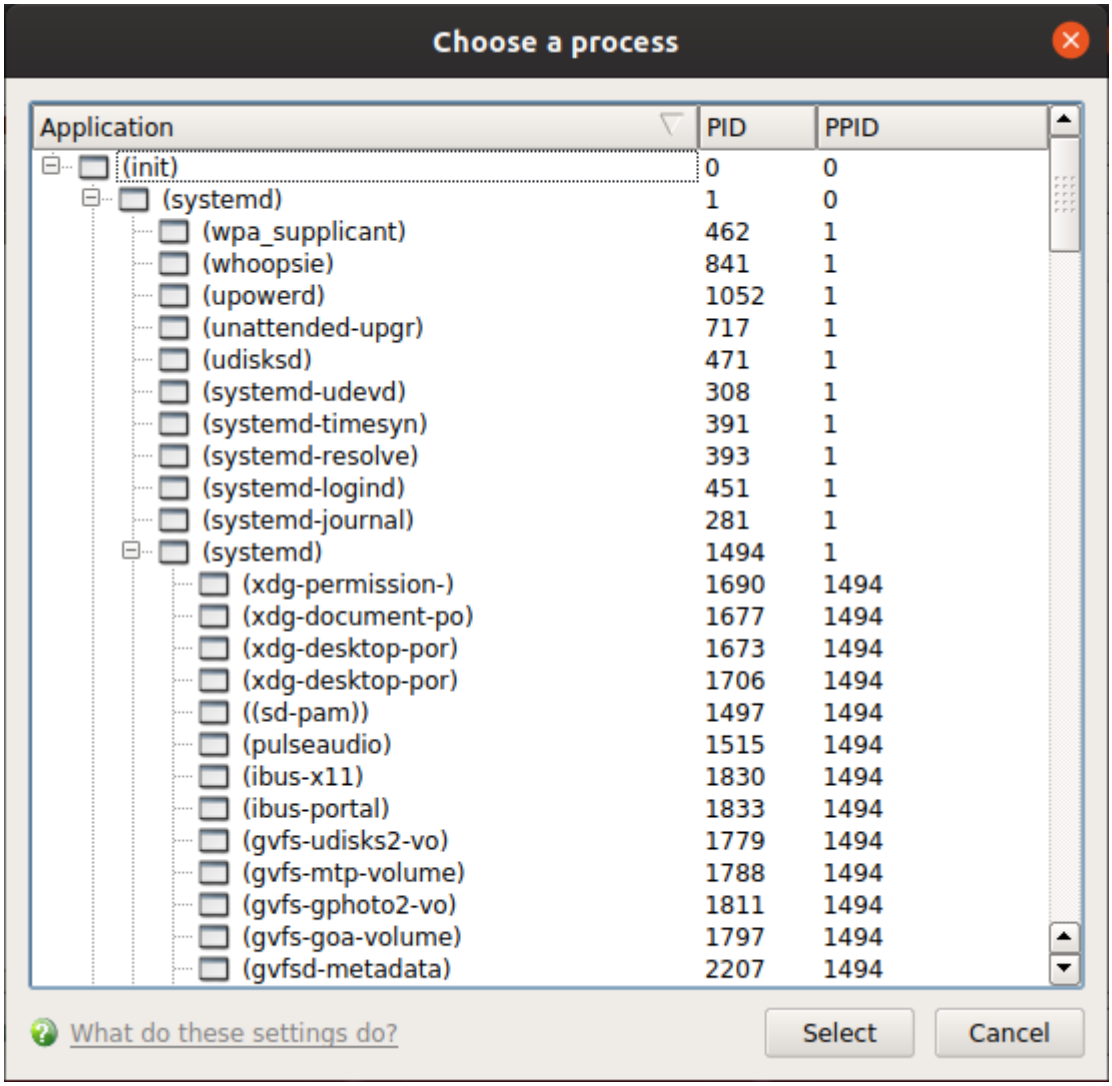
- Click the 'Add' button.
- There are two ways to choose the application that you want to exclude:



Browse Files... - Navigate to the file / folder you want to exclude in the left pane and move it to the right pane by clicking the right arrow:



Browse Running Processes - Choose the target application from a list of processes running on your PC. The parent file of the process is added to exclusions.



- Repeat the process to add more exclusions.
- Click 'OK' to register your exclusions.