How to run on-demand and scheduled antivirus scans in CCS on Mac OS devices

Click 'Antivirus' > 'Run a Scan'

- CCS leverages multiple technologies, including real-time monitoring and on-demand scans, to keep endpoints totally free of malware
- You can scan any folders, files, drives or any area on your device any time for malware
- You can also create your own scan profiles to scan specific files, folders and drives and schedule scans to run at a specific time
- CCS shows the list of items identified as malware at the end of each scan. You can choose to ignore or clean the infected files.

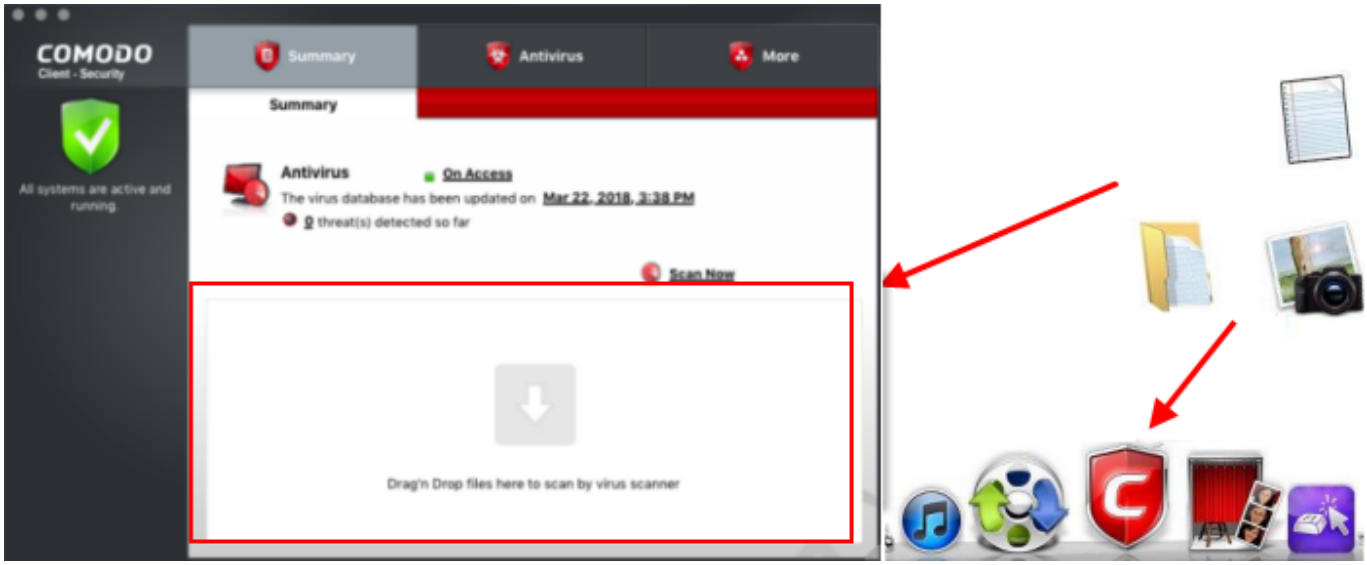
Click the links below to jump to the task you need help with:

Instantly scan files and folders

- Drag and drop the individual files, folders or drives into the scan box to instantly check whether they contain threats.
- For example, this is useful if you are wary about an item you have copied from an external source or downloaded from the internet.

Instantly scan an item

- Drag the item into the scan box in the 'Summary' interface



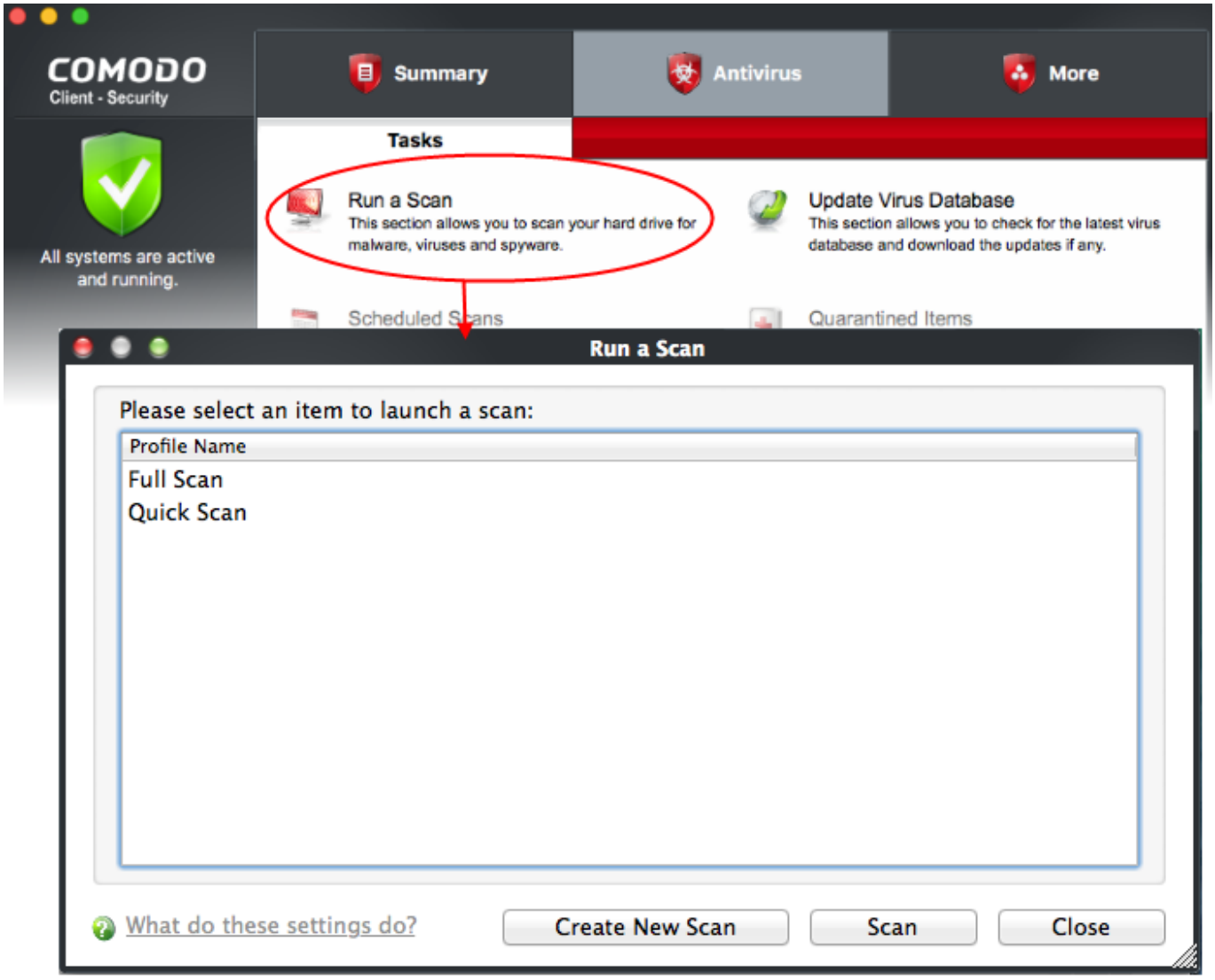
The item is scanned immediately.

Note - CCS skips files which are larger than the max. size allowed. Click 'Antivirus' > 'Scanner Settings' > 'Manual Scanning' to view this threshold. See this wiki to read more on scanner settings.

- Scan results are shown when completed. See Scan Progress and Results for help to view results and handle identified threats.

Run an on-demand virus scan

- Click the 'Antivirus' tab then 'Run a Scan'



- Choose a scan profile to select the areas you want to scan:
- CCS ships with a set of pre-defined profiles:
    - **Full Scan** - Scans every drive, folder and file on your system, including external connected devices
    - **Quick Scan** - Scans areas prone to attack, like important operating system files, system memory and auto-run entries.
    - You can also create user defined profiles to scan desired areas of your computer. See 'Create a custom scan' if you need help to do this.
- Click 'Scan'.

Note - CCS skips files which are larger than the max. size allowed. Click 'Antivirus' > 'Scanner Settings' > 'Manual Scanning' to view this threshold. See this wiki to read more on scanner settings.

- Next - Scan progress and results

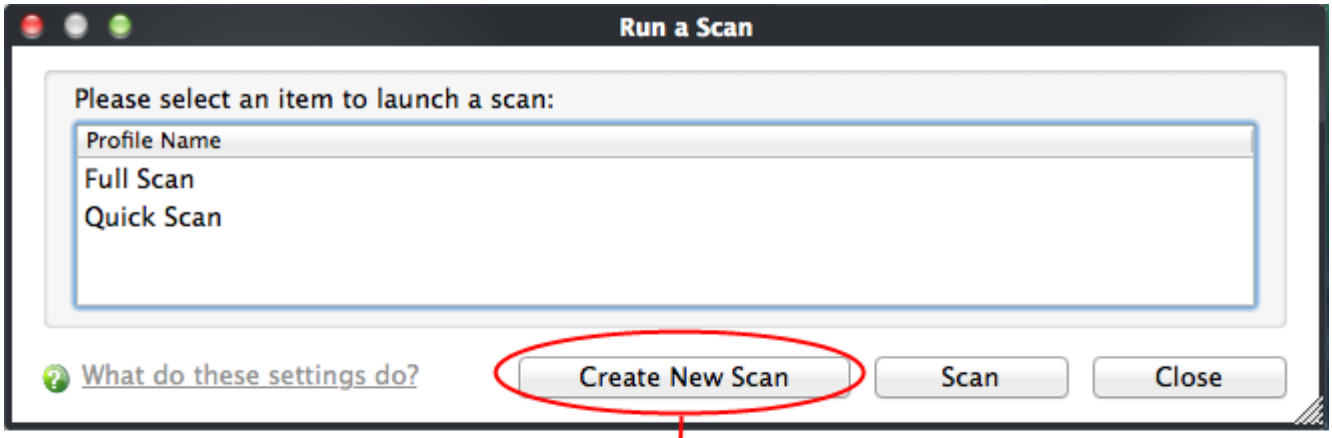
Create a custom scan profile

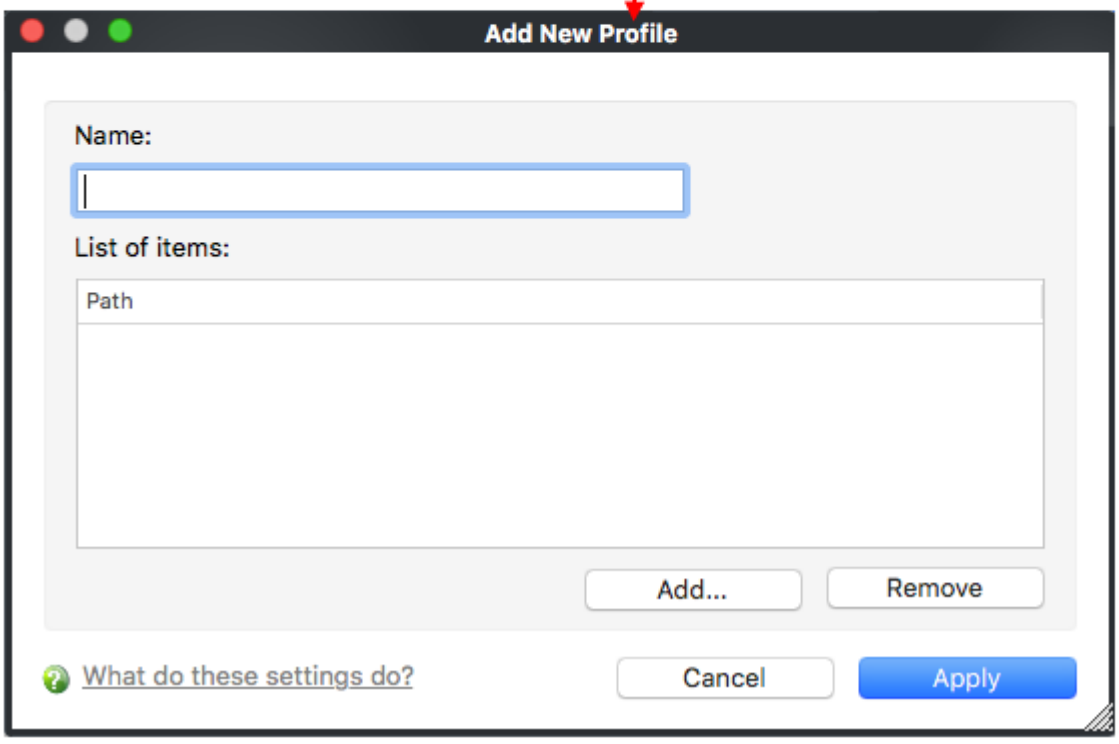
Click 'Antivirus' > 'Run a Scan' > 'Create New Scan'

- 'Scan Profiles' let you set up custom scans on specific areas on your system. Scan profiles can be run on-demand at any time.
- You can also add a custom scan profile to a schedule to periodically run the scans at specified intervals.

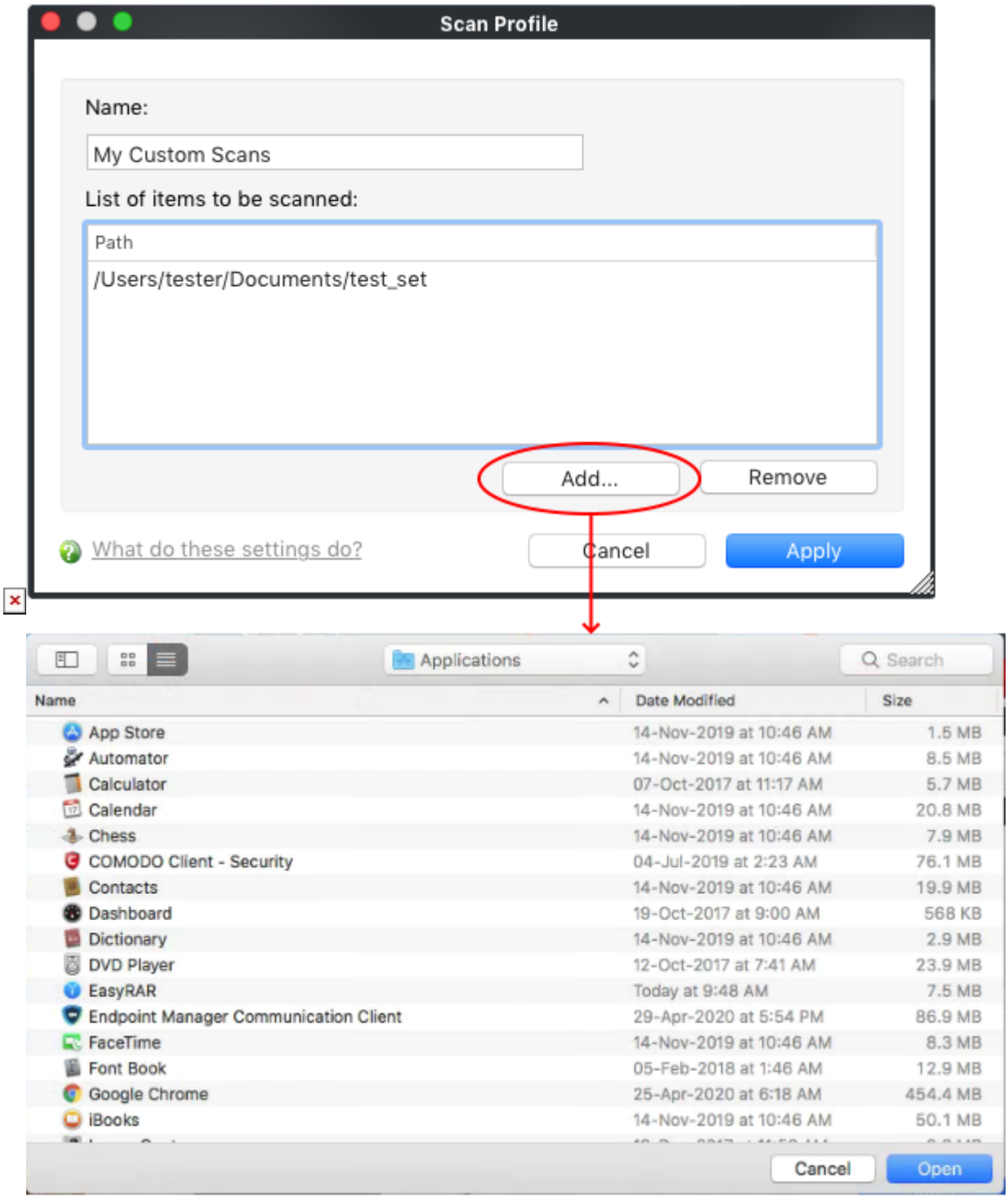
Create a new scan

- Click the 'Antivirus' tab then 'Run a Scan'
- Click the 'Create New Scan' button





- **Name** - Enter a label for the scan profile. For example, 'My Custom Scans'
- Click 'Add' to select the items you wish to include in the scan



- Select the item and click 'Open'
- Repeat the process to add more items
- Click 'Apply' in the scan profile dialogue.
- The profile is added to the list of scan profiles and available for selection while running an on-demand scan.
- Repeat the process to add more scan profiles.

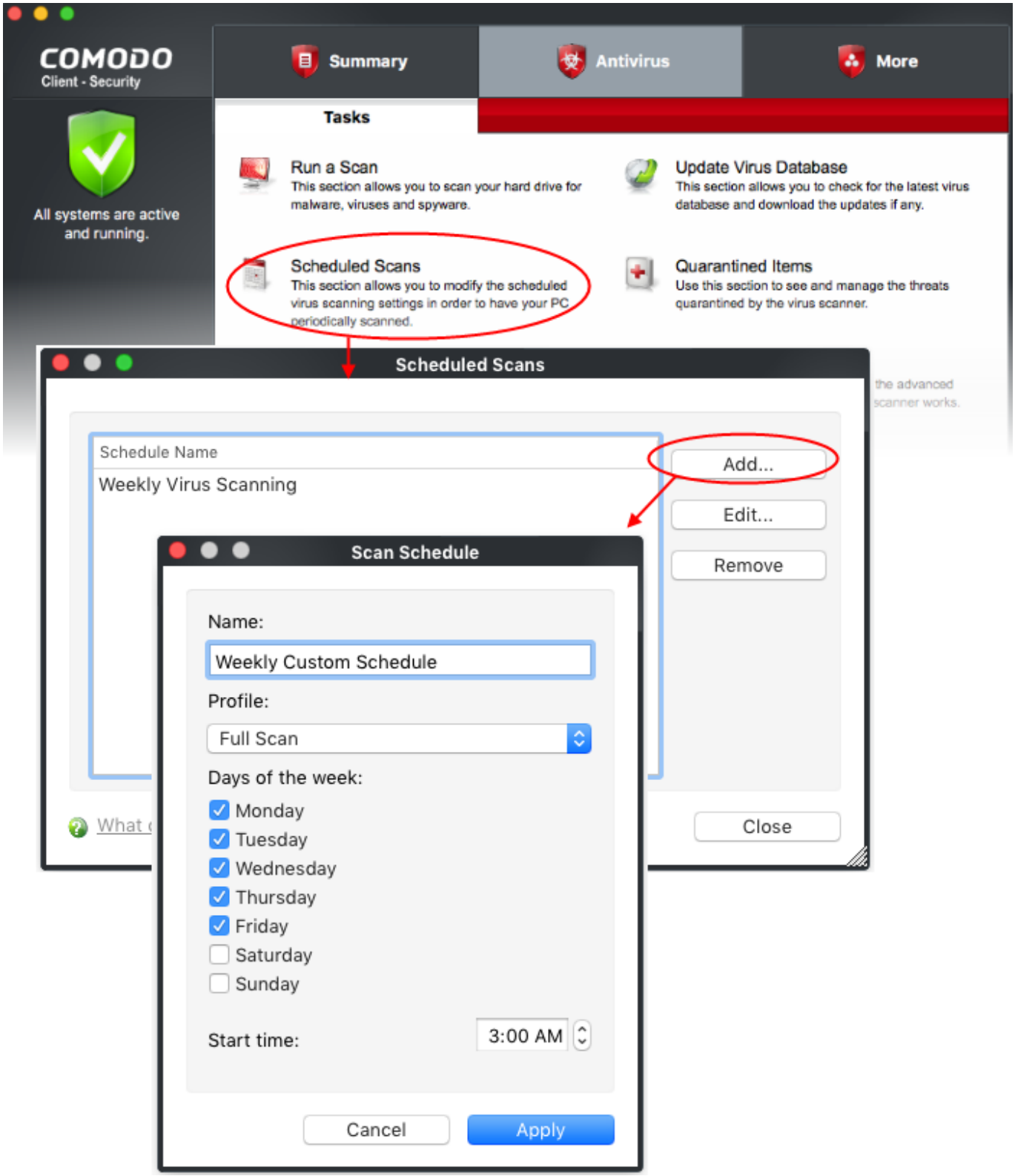
Create a scheduled scan

Click 'Antivirus' > 'Scheduled Scans' > 'Add'

- The highly customizable scheduler lets you timetable virus scans according to your preference.
- You can schedule a scan of your entire computer or specific areas. You can create an unlimited number of schedules.
- You can run scans at daily, weekly, monthly or custom intervals.

Create a scan schedule

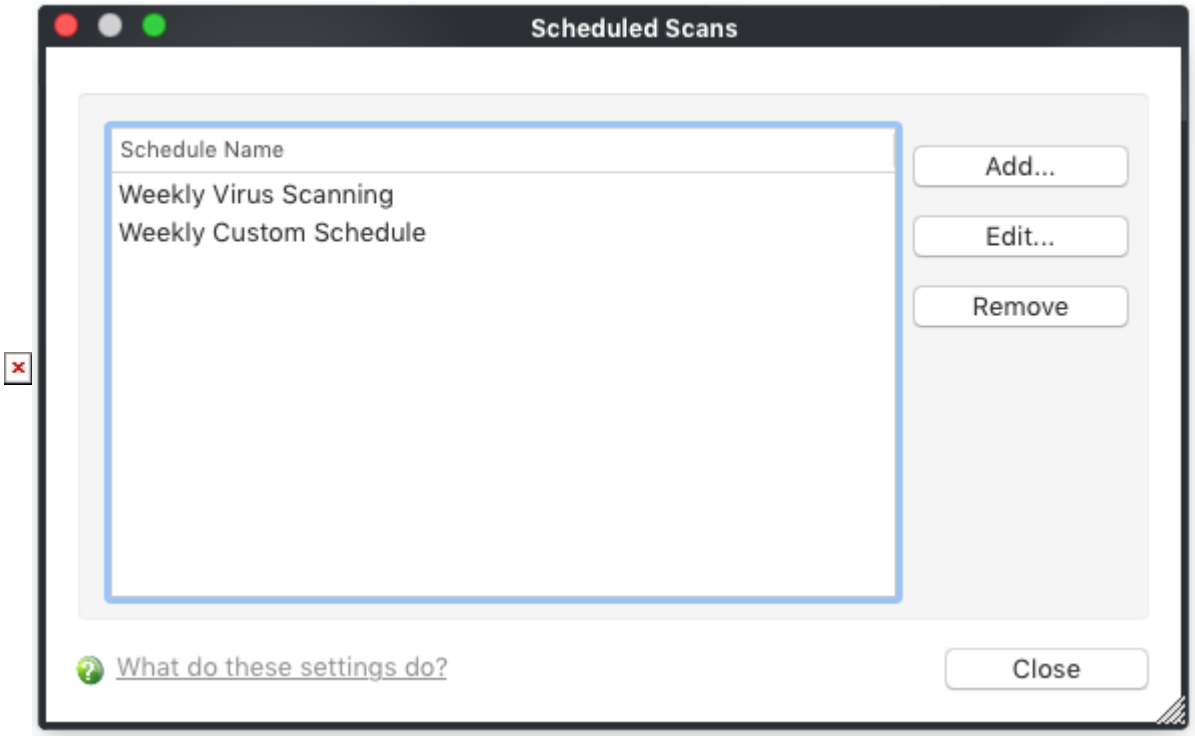
- Click 'Antivirus' tab > 'Scheduled Scans'
- Click the 'Add' button in the 'Scheduled Scans'



- Configure your schedule:
    - **Name** – Enter a label for the new schedule. E.g. 'Daily scan of external devices'
    - **Profile** – The profile determines which areas of your computer are scanned. 'Full Scan' and 'Critical Areas' are the default options. You can also create your own profile of specific targets. See Create a custom scan profile if you need help to do this.
    - **Days of the week** – Select the weekdays the scan should run.

- **Start time** – Select the time the scan should start on the specified weekdays

- Click 'Apply'



- Repeat the process to create more scan schedules.

- Click 'Close' to save the schedule.

CCS will run the scans on specified time and show the results at the end of each scan. The results are shown only if 'Automatically quarantine threats found during scanning' is disabled in scheduled scanner settings: 'Antivirus' > 'Scanner Settings' > 'Scheduled Scanning'. See this wiki to read more on scanner settings.

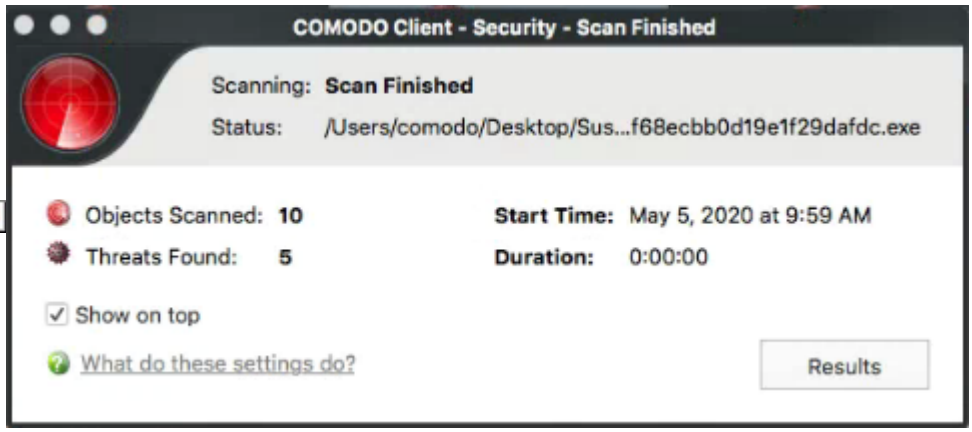
Scan progress and results

- Before running the scan, xcitium Client Security checks for antivirus database updates. If updates are available they are downloaded and installed.

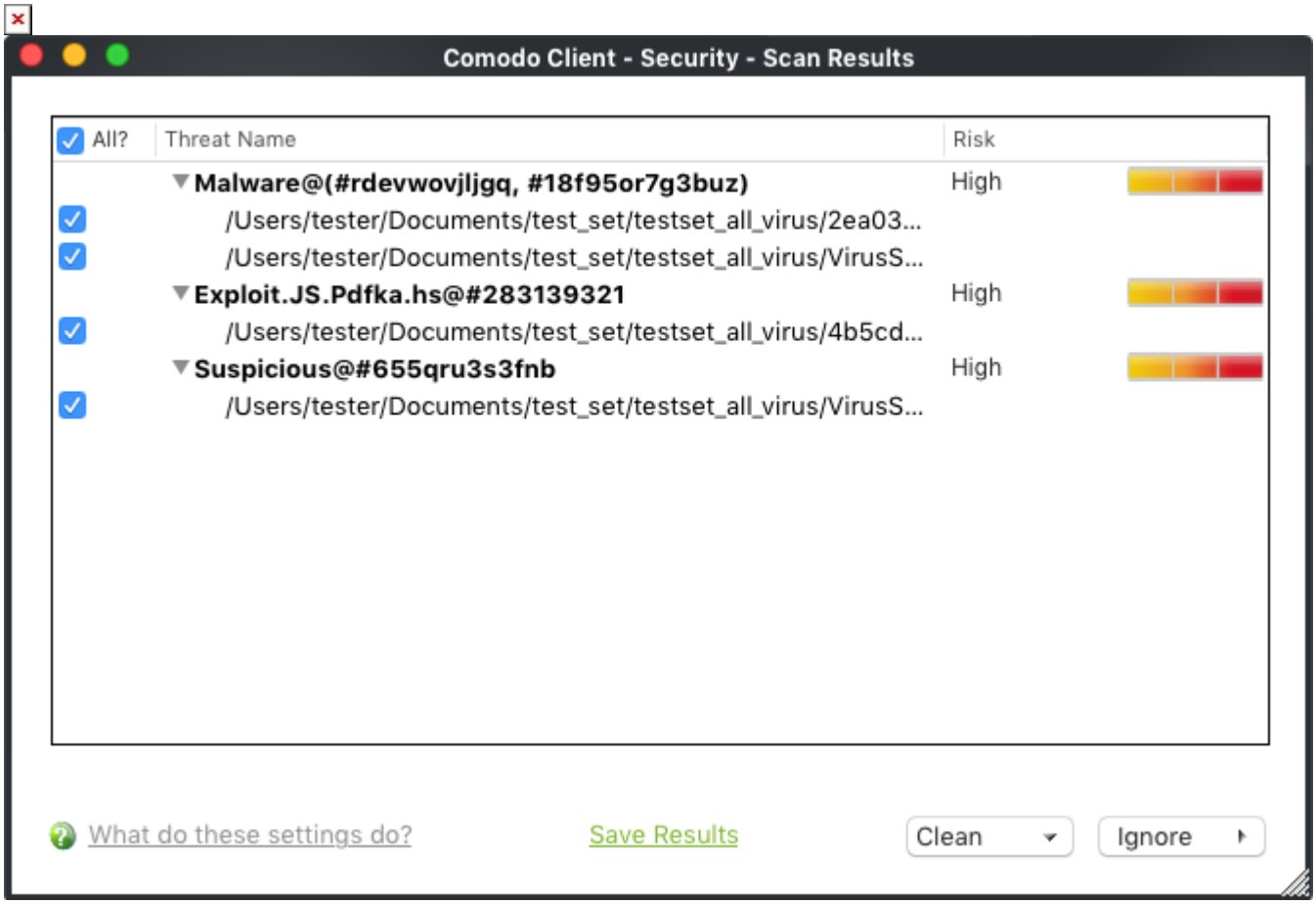
The scan, based on the profile you selected, will begin immediately.

The progress dialogue shows the profile name, the location that is currently being scanned, the start time and duration of the scan, the total number of objects scanned so far, and the number of threats found:

Results are shown at the end of the scan:



- Click the 'Results' button to see detailed file information.
- The results window lists all threats discovered by the scan and provides controls which let you deal with them:



- The buttons at the bottom of the results window let you take action on the selected threats:

- **Clean** - Use the drop-down menus to apply actions to files:

  - **Clean** - Removes the infection and retains the original file. If no routine exists, CCS will move the file to quarantine. Click 'Antivirus' tab > 'Quarantined Items' to view this area. You can restore or permanently delete files from quarantine as required. See Manage Quarantined Items if you need help with these options.

  - **Disinfect** - If a disinfection routine exists, CCS will remove the virus and keep the original file. If not, the file will be quarantined.

  - **Quarantine** - Malicious items will be moved to quarantine. You can review quarantined items and delete them permanently or restore them. See 'Manage Quarantined Items' for more details.

- **Ignore** - Use the drop-down menus to apply actions to files:

  - **Once:** Allows the file to run this time only. Removes the item from the threat results. The file isn't added to the exclusion list and is flagged as threat by the next scan.

  - **Add to Exclusions:** Add an item to the exclusions list and skipped it by future scans and not consider it to be a threat. You can review exclusions at 'Click 'Antivirus' tab > 'Scanner Settings' > 'Exclusions'. See 'Exclusions' in this wiki to read more.

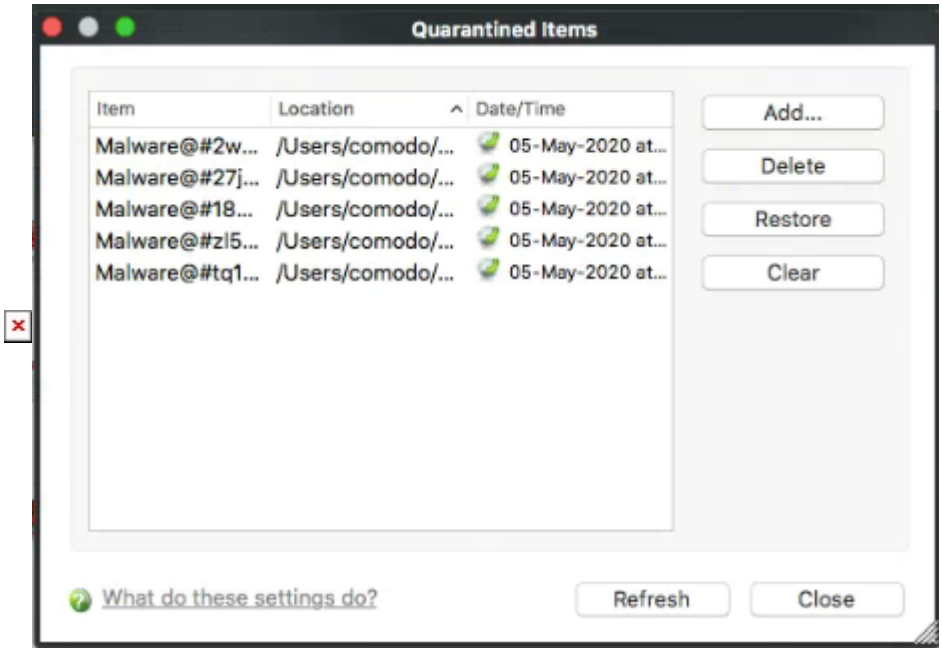
Manage quarantined items

Click 'Antivirus' > 'Quarantined Items'

- Quarantine is an encrypted holding area for threats detected by the antivirus scanner

- Quarantined files cannot be executed, so they present no danger to your computer or data

- You can analyze the trustworthiness of these items and take actions like permanently remove them from your computer or restore them to their original location.



- **Item** - The name of the malicious application or process
- **Location** - The file path of the item
- **Date/Time** - Date and time the item was moved to quarantine.

The interface lets you review quarantined files and take the following actions:

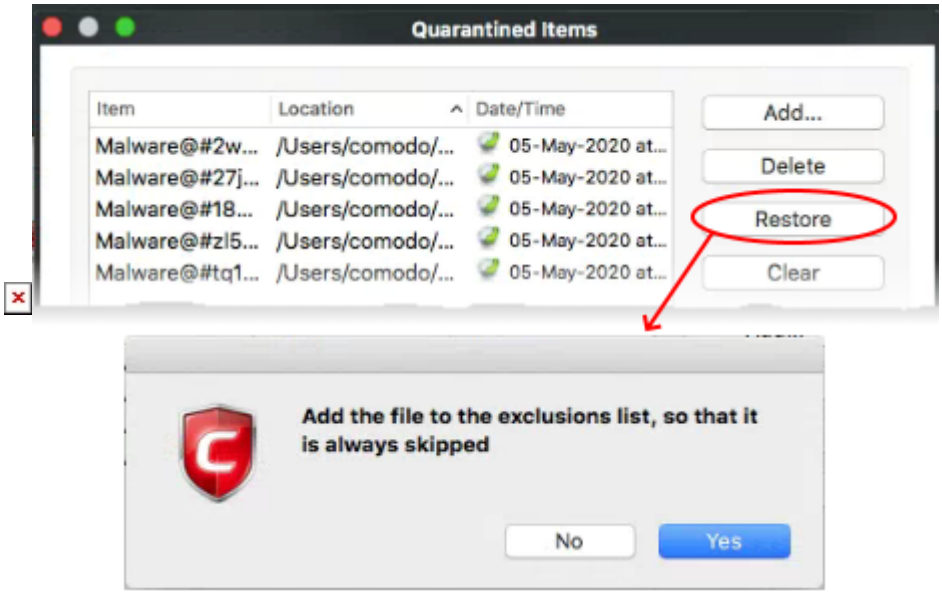
- Permanently delete the file
- Restore the file to its original location

Remove a quarantined item

- Click 'Antivirus' > 'Quarantined Items'
- Select the items in the quarantine interface and click the 'Delete'
- Click 'Clear' button to delete all the quarantined items permanently.
- The files are deleted from your computer

Restore a quarantined item

- Click 'Antivirus' > 'Quarantined Items'
- Select the items to be moved back to their original locations and click the 'Restore'



You will be asked if you want to add the item to the Scan Exclusions list:

- **'Yes'** - The file is restored to its original location. It is not flagged as dangerous nor quarantined by future antivirus scans. You can manage excluded items in the Scanner Settings interface ('Antivirus' > 'Scanner Settings' > 'Exclusions'). See 'Exclusions' in this wiki to read more.

- **'No'** - The file is restored to its original location. If the file contains malware it will be re-quarantined by the next antivirus scan.