Click ‘Configuration Templates’ > ‘Profiles’ > open a Windows profile > open the ‘Containment’ section

What is the container?

- The 'Container' is a secure, virtual environment in which Comodo Client Security (CCS) runs unknown files.
- Files in the container cannot cause damage because they are isolated from the operating system, file system, and user data.
- Programs in the container run as normal from the end-users point of view, so there is no interruption to their usual work-flows.
    - You can also create rules to auto-contain files at specific restriction levels.
    - Modifications to containment settings are logged. You can view the old and new values in the 'Dashboard' > 'Audit Logs' screen.
- You can configure the overall behavior of the container and the virtual desktop in the containment section of a profile

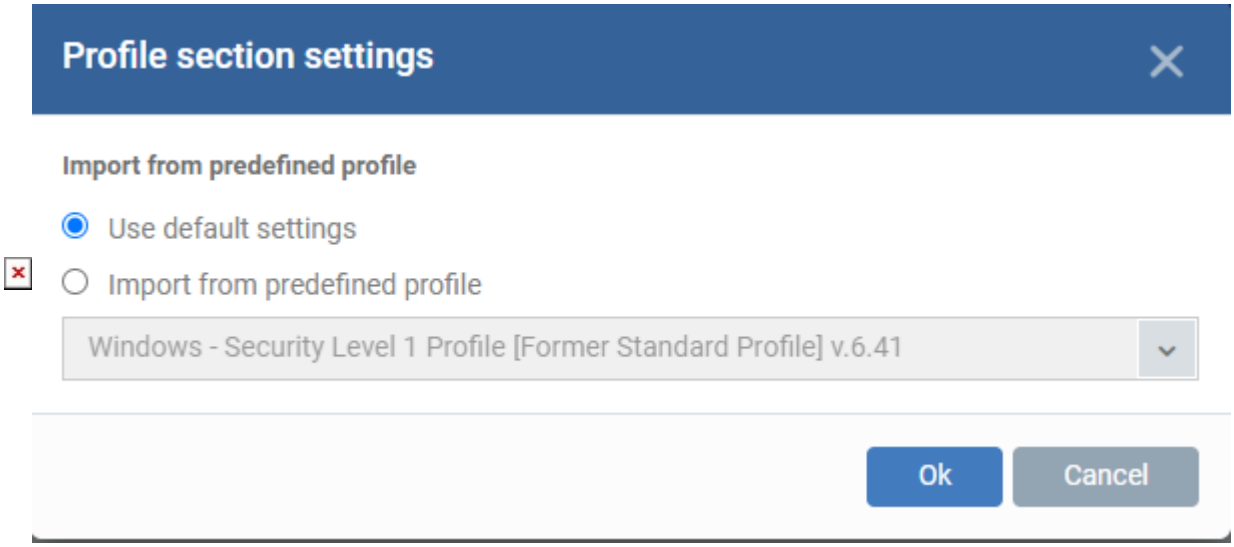
Configure containment settings

- Login to ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click ‘Configuration Templates’ > ‘Profiles’
- Open the Windows profile applied to your target devices
    - Open the 'Containment' tab

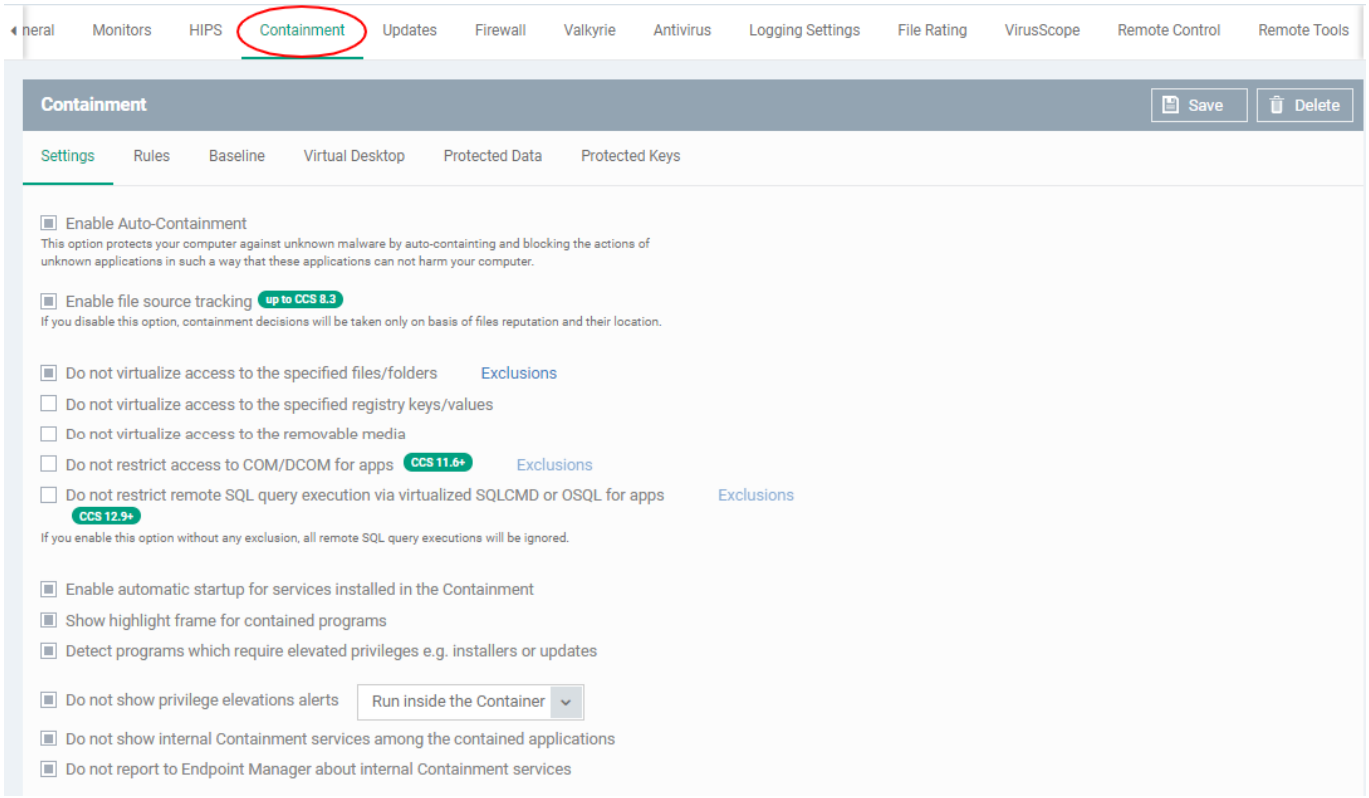
      OR
    - Click 'Add Profile Section' > 'Containment', if it hasn't yet been added:

- You must restart the target endpoints if you add a containment section to a profile.
- Click 'Confirm' to continue.

You can use the default containment settings or import them from a predefined profile:



The containment settings screen opens:



The containment section has four tabs. Click the following links for help with each area:

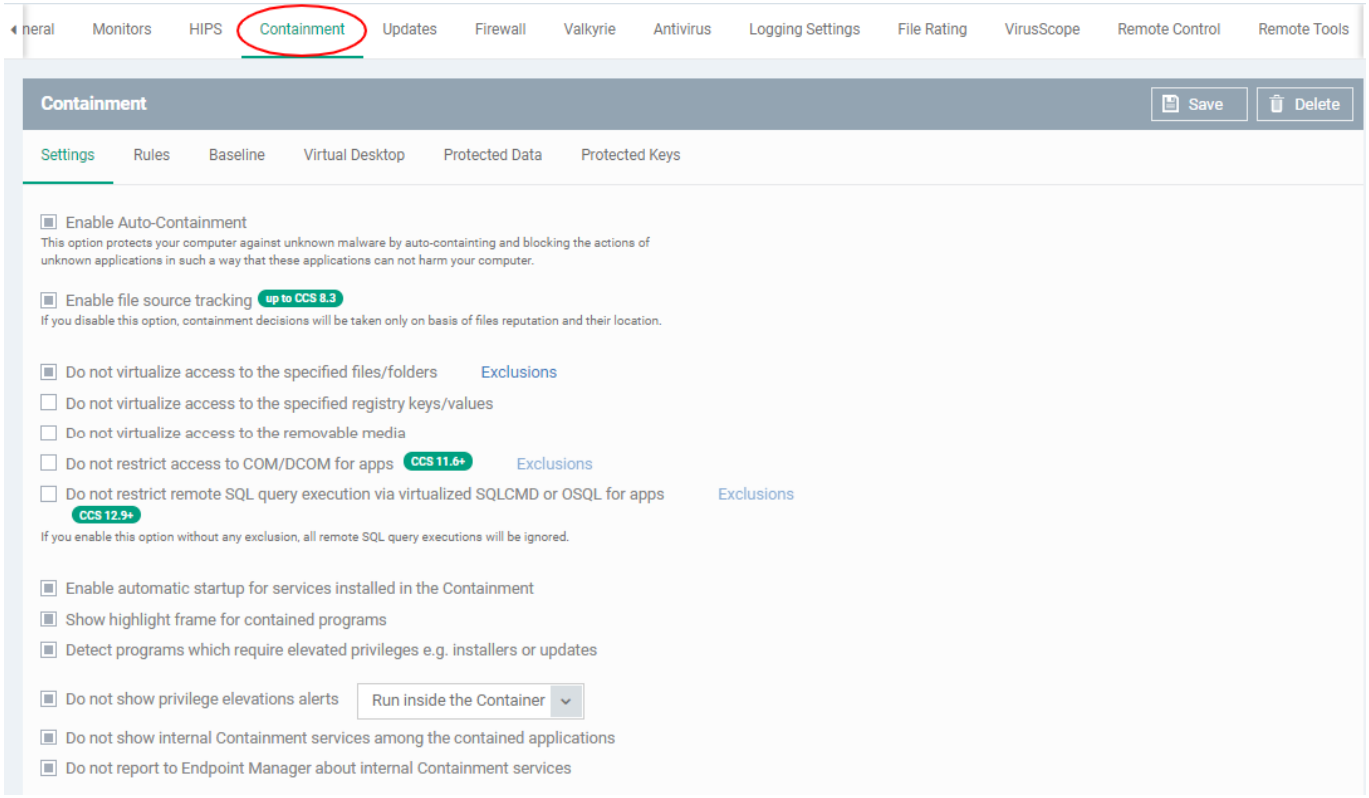
- General settings
- Rules

- Baseline settings
- Virtual Desktop

General settings

General preferences for the overall behaviour of the container.

- Click the 'Settings' tab in the containment configuration screen:



- **Enable Auto-Containment** - Activate or deactivate auto-containment on the endpoint. If enabled, CCS will automatically run unknown applications inside the container. You can also create rules to fine-tune exactly which types of files are contained. (Default = Enabled)
- **Enable file source tracking** - If enabled, CCS will consider the origin of a file when deciding whether to contain it or not.
    - For example, if you only want to auto-contain files downloaded from the internet, then 'internet' is your source.
    - If this setting is disabled then the source is disregarded. Only the reputation and location of the file are considered.
    - Applies only to CCS versions 8.3 or lower.

      (Default = Enabled)
- **Do not virtualize access to the specified files/folders** - Contained applications write to a virtual file system, preventing them from potentially damaging files on the host. This setting lets you define

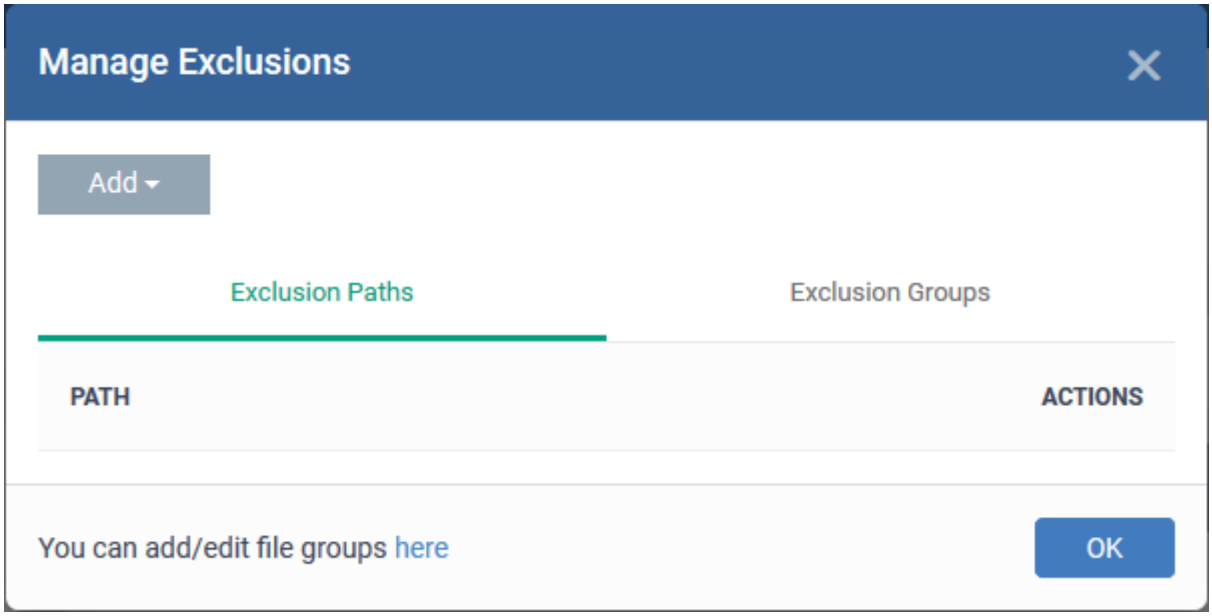
exceptions to that rule. You can specify folders or files on the host system which contained applications are allowed to access. (Default = Enabled)

Access scope if enabled:

- **Data files** (.doc, .txt etc) – Read/Write/Rename/Delete. Useful, for example, if you want MS Word in the container to save changes to a .doc file on the host file system.

- **Executable files** (.exe, .msi etc) – Rename/Delete only.

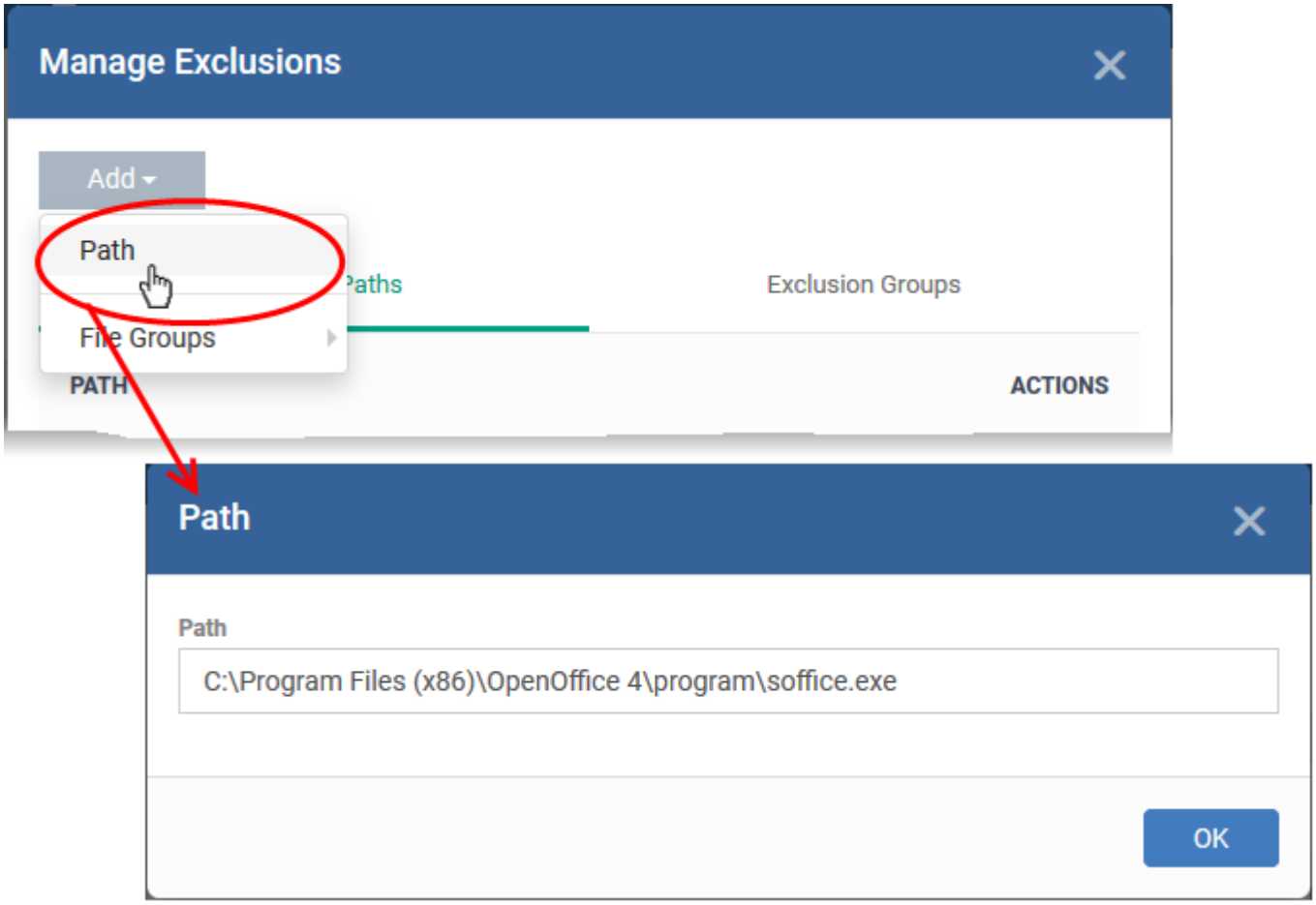
Enable 'Do not virtualize access to the specified files/folders', then click 'Exclusions':

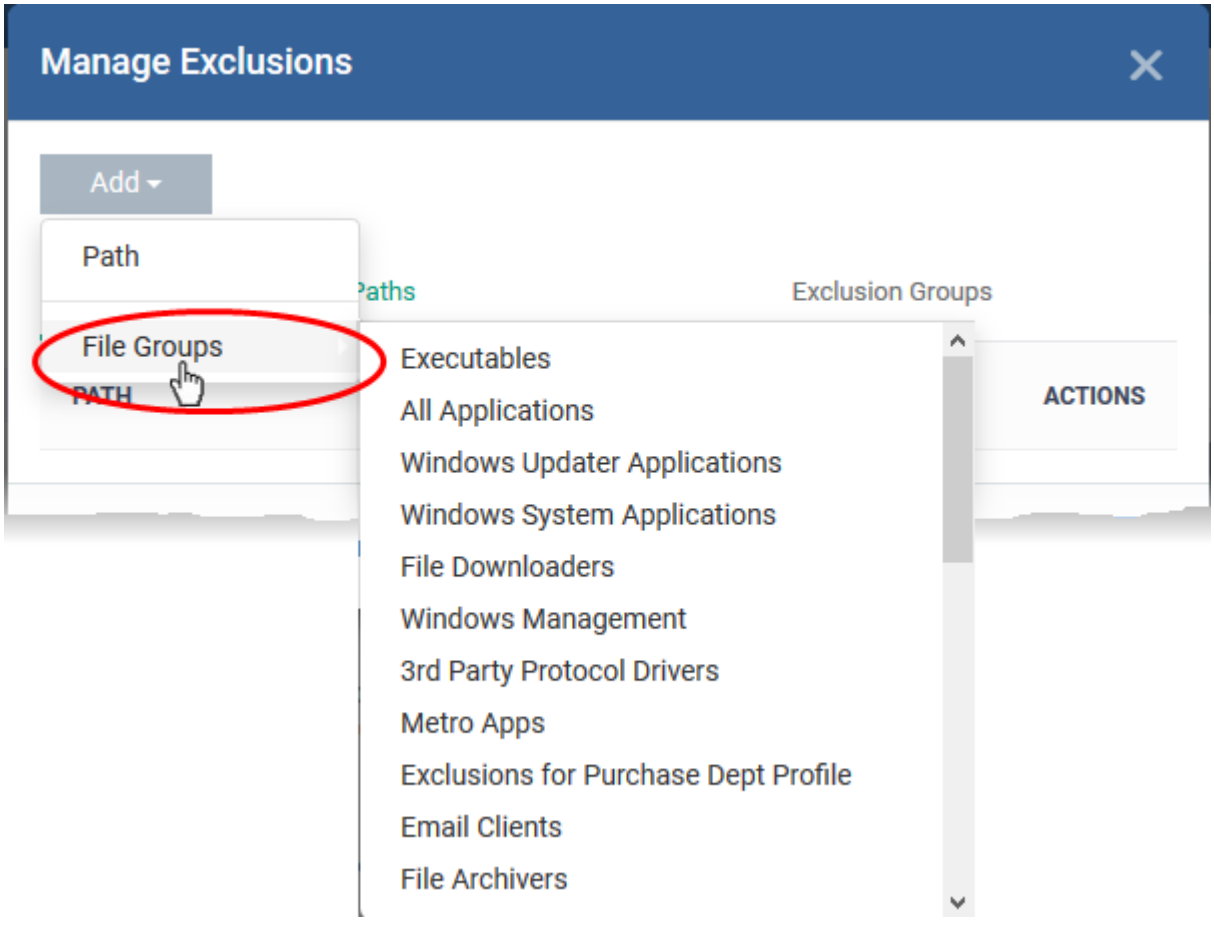


- **Exclusion Paths** – Enter the location of an individual item that you want to exclude. Contained files can write to the files/folders you specify here. You can add multiple files by clicking ‘Add’ again.

- **Exclusion Groups** – Allow contained apps to access apps and files in a particular group. A file group is a collection of file types which have similar attributes, scope, or functionality. For example, ‘Executables’, ‘Metro Apps’, or ‘Windows System Applications’.

Click ‘Add’ then 'Path’ or ‘File Group’ as required:

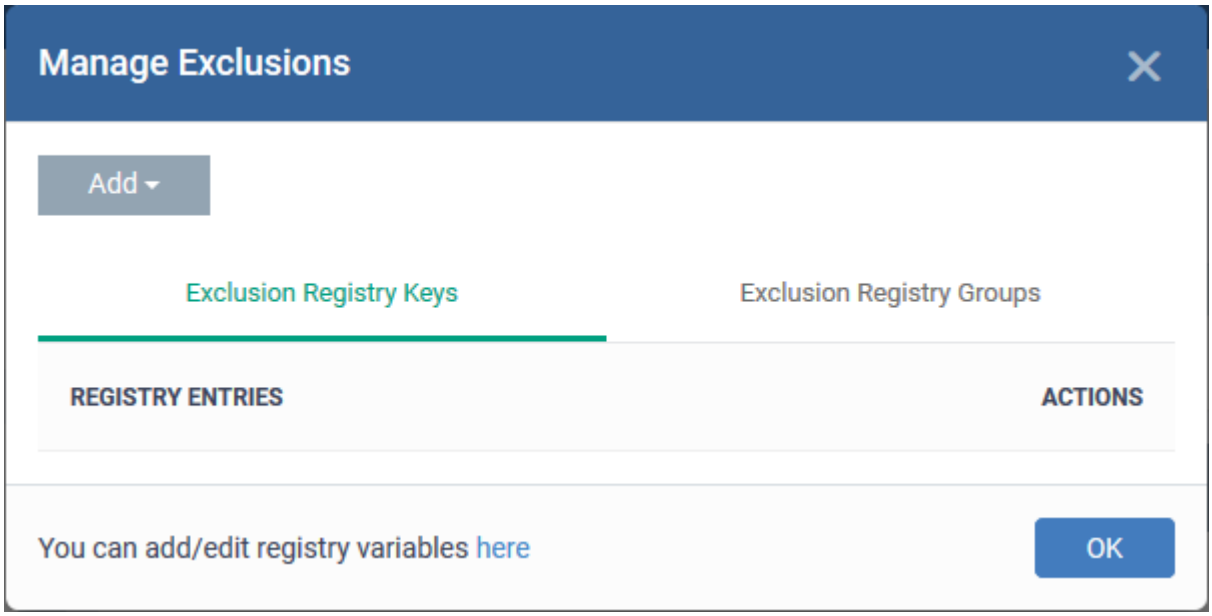

Manage Exclusions
Add
Path
File Groups
Paths
Exclusion Groups
PATH
ACTIONS
Path
Path
C:\Program Files (x86)\OpenOffice 4\program\soffice.exe
OK


Manage Exclusions
Add
Path
File Groups
Paths
Exclusion Groups
PATH
ACTIONS
Executables
All Applications
Windows Updater Applications
Windows System Applications
File Downloaders
Windows Management
3rd Party Protocol Drivers
Metro Apps
Exclusions for Purchase Dept Profile
Email Clients
File Archivers

Click 'OK' to save your settings.

- **Do not virtualize access to the specified registry keys/values** - Contained applications can access registry keys and values on the local system but cannot save any changes to them. This setting lets you define exceptions to that rule. Contained applications will be able to access and save changes to registry items.

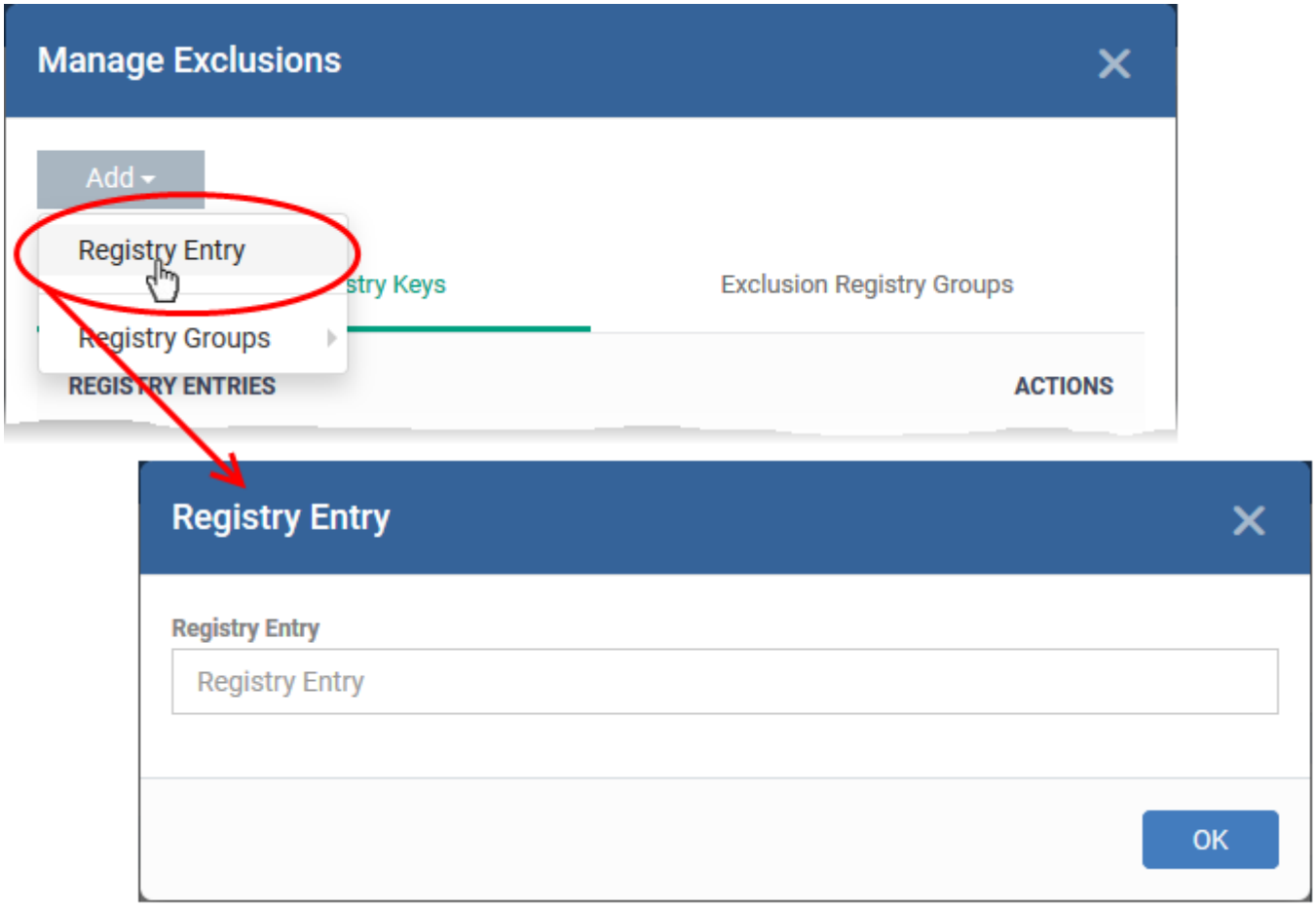
    - Enable 'Do not virtualize access to specified registry keys/values' and click 'Exclusions' beside it:



- **Exclusion Registry Keys** - Enter the location of an individual key that you want to exclude. Contained files can write to the keys you specify here. You can add multiple keys by clicking ‘Add’ again.

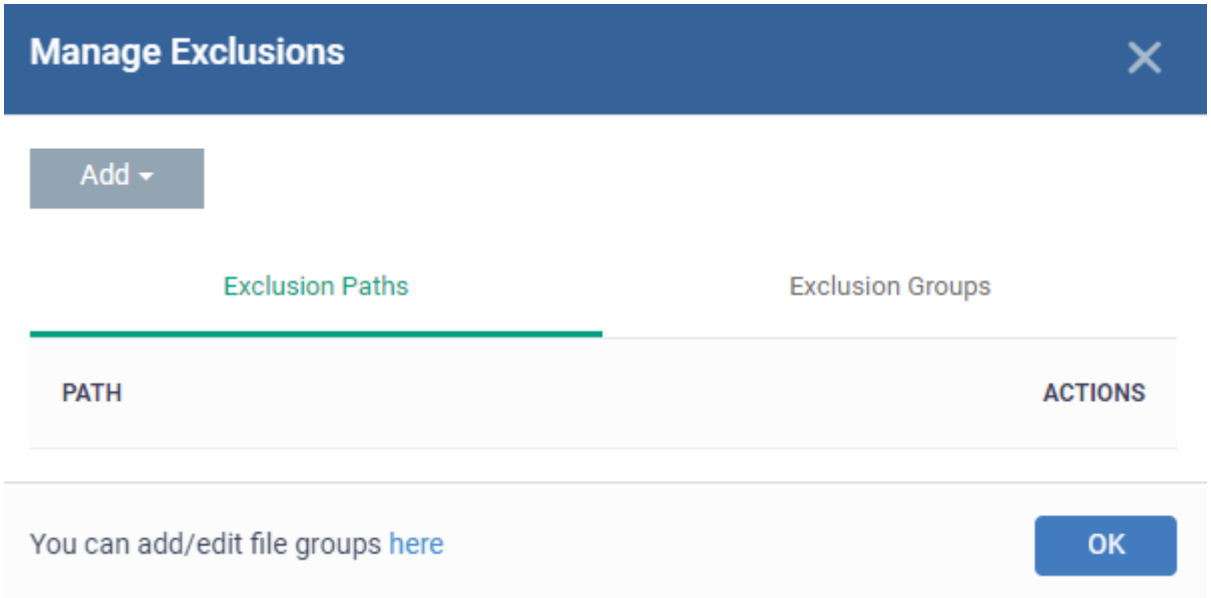
- **Exclusion Registry Groups** - Allow contained applications to access all keys in a particular group. A registry group is a collection of keys with similar scope or functionality.

Click ‘Add’ then 'Registry Entry’ or ‘Registry Group’ as required:

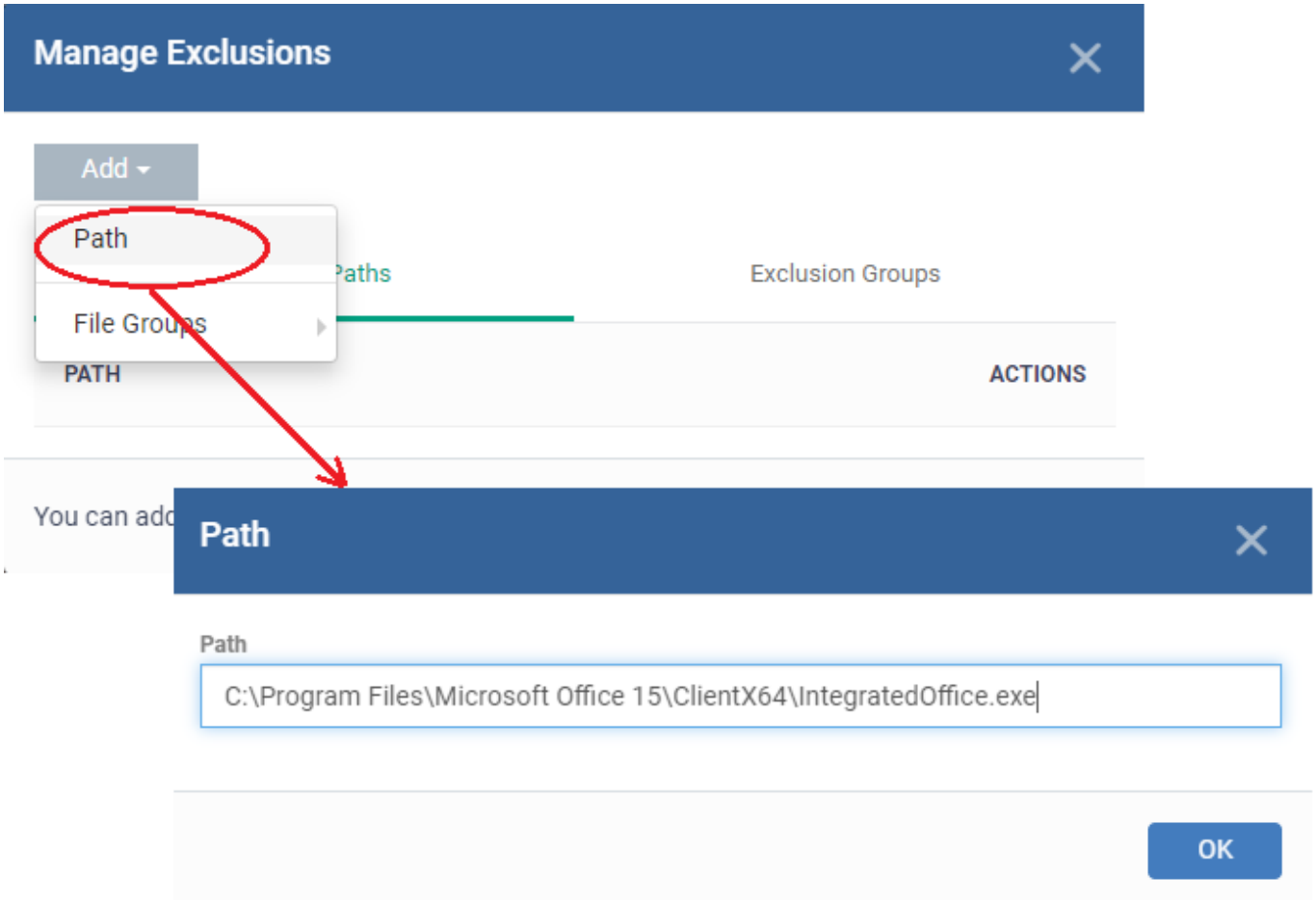


Click 'OK' to save your settings.

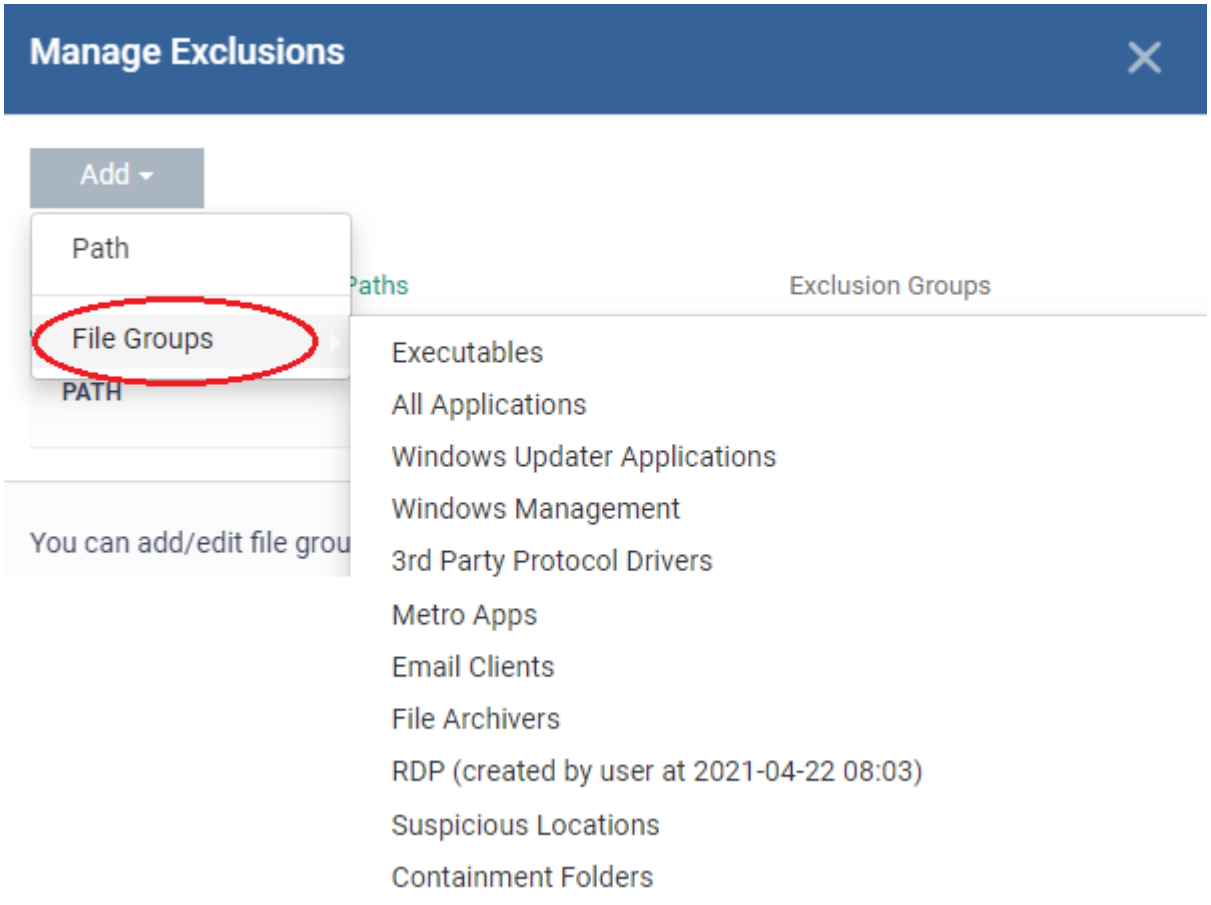
- **Do not virtualize access to removable media** - Allow contained applications to write to external storage devices like USB sticks and external hard disk drives. (Default = Disabled)
    - By default, applications in the container can only save data to a folder called 'Shared Space'. Users can save data to this folder if they want to access it from the host system.
    - This setting provides another way to export data from the container or virtual desktop.
- **Do not restrict access to COM/DCOM for apps -**Component Object Model (COM) is Microsoft's object-oriented programming model that defines how objects interact within a single application or between applications - specifying how components work together and inter-operate.
    - By default, contained applications are prohibited from accessing the COM or Distributed COM (DCOM) components currently running on a device.
    - If required, you can create a list of applications, that can access the COM and DCOM components, even if the application is run inside the container.
    - Enable 'Do not restrict access to COM/DCOM for apps' and click 'Exclusions' beside it: (Default = Disabled)



- The 'Manage Exclusions' dialogue will appear with a list of defined exclusions under two tabs:
    - **Exclusion Paths** - Enter the location of an individual item that you want to add. The application you specify here can access COM / DCOM components when run inside the containment.
    - **Exclusion Groups** - Allow applications in a particular group to access COM / DCOM interfaces. A filegroup is a collection of file types that have similar attributes, scope, or functionality. For example, ‘Executables’, ‘Metro Apps’, or ‘Windows System Applications. Endpoint Manager ships with a set of pre-defined file groups. You can create custom file groups from the 'Settings' > 'System Templates' > 'File Groups Variables' interface.
- Click ‘Add’ then 'Path’ or ‘File Group’ as required:



- Click 'Ok'



- **Do not restrict remote SQL query execution via virtualized SQLCMD or OSQL for apps -** The

SQL script execution via virtualized osql and sqlcmd should be blocked. This option should be disabled by default for all predefined profiles. Exclusions should act the same as all other exclusions.

- If you enable this option without any exclusion, all remote SQL query executions will be ignored. Click here to know how to add or manage exclusions.

- **Enable automatic startup for services installed in the Containment** - By default, the CCS permit contained services to run at Windows startup. On disabling this check-box contained services do not run on target endpoints. (Default = Enabled)

- **Show highlight frame for contained programs** - Shows a green border around programs running in the container. (Default = Enabled)

- **Detect programs which require elevated privileges e.g. installers or updates** - CCS proactively tracks programs that require admin privileges to run.

  - A program that is allowed to run with elevated privileges is permitted to make changes to important areas of the endpoint, such as the registry.

- **Do not show privilege elevation alerts** - If 'Detect...' is enabled (see setting above), then an alert is shown to end-users when an unknown/new program requires elevated privileges to run. Enable this setting if you do not want these alerts to be shown (Default = Enabled). Instead, CCS will implement the action you choose in the drop-down menu:

- **Do not show internal Containment services among the contained applications** - The 'View Active Processes' interface has an option which lets you view a list of contained processes. This setting lets you exclude processes started by Comodo client software from that list.

  You can view contained processes in CCS as follows:

  - Click 'Tasks' > 'General Tasks' > 'View Active Processes'

  - Right-click anywhere in the interface > select 'Show Contained only'

- **Do not report to Endpoint Manager about internal Containment services** - Info about Comodo client processes running in the container is not sent to Endpoint Manager. Client processes are those started by CCC or CCS themselves.

  - Click 'Security Sub-Systems' > 'Containment' in EM console to view a history of contained applications and processes.

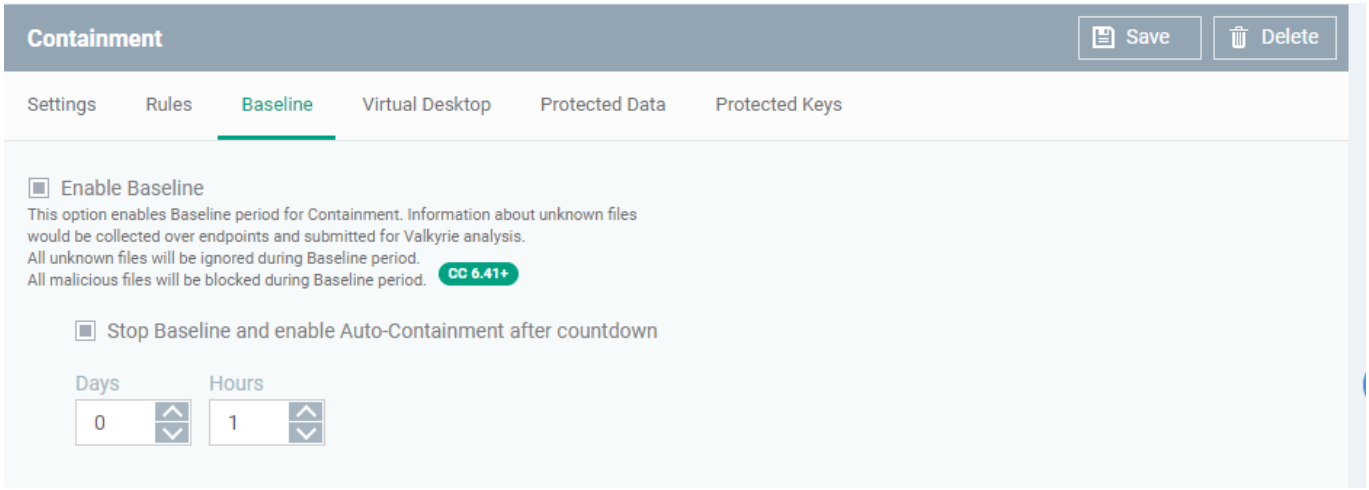
Rules

- Containment rules determine whether a program should run in the virtual environment, run as normal, or run with restrictions. CCS consults these rules every time a program is opened on the endpoint.

- Containment rules are covered in detail in their own wiki at https://wiki.itarian.com/frontend/web/topic/how-to-create-auto-containment-rules-in-a-windows-profile

Baseline settings

- A baseline is a limited period of time during which unknown files are not contained.
- This feature is best used during the initial setup period when, typically, many unknown files are discovered on a network.
- All unknown files discovered during this period are uploaded to Valkyrie, Comodo's file analysis service. Valkyrie tests each file and reports back to Endpoint Manager on whether the file is safe or malicious.
- During this time period, all the unknown files are ignored and malicious files are blocked.
- Safe files are allowed to run as normal on the host in future, while malicious files are quarantined.
- The system lets admins quickly whitelist all 'unknown-but-safe' files on their network, leading to a smoother roll-out.
- After the baseline period is over, auto-containment should be re-enabled. All unknown files going forward will be run in the container.



- **Enable Baseline** – Switch on the baseline feature
- **Stop Baseline and Enable Auto-Containment after countdown**:
  - **Enabled** - Baselining lasts the length of time you set in the fields. Auto-containment will resume when this period expires. 5 working days is recommended for networks.
  - **Disabled** - Baselining will continue until you disable it in the setting at the top.

The timer begins after you apply the profile to your network.

- Click 'Save' to apply your changes.

The Virtual Desktop

- The virtual desktop is a standalone sandbox environment in which you can run Windows programs and internet browsers. The virtual desktop uses the same virtualization technology as the container.
- Programs in the virtual desktop are isolated from the rest of the host, preventing them from causing damage.
- You can set the virtual desktop to start automatically when a selected user logs in to a device. This makes the virtual desktop the default environment for the user, instead of the host operating system.
- All programs and services run exactly as they would under Windows, making the system completely transparent.
- Virtual desktop settings are covered in their own wiki at https://wiki.itarian.com/frontend/web/topic/how-to-configure-virtual-desktop-settings-in-a-windows-profile

Further reading

How to configure virtual desktop settings in a Windows profile

How to create auto-containment rules in a Windows profile