How to configure external device control in CCS for Linux

Open CCS for Linux > Click ‘More’ > ‘Preferences’ > ‘Device Control’

- Device control lets you prevent external devices from connecting to managed Linux endpoints. Enabling this setting will, for example, block access to USB sticks and external drives.
- You can define exclusions for selected devices. The selected devices will be allowed to connect, but all others will be blocked.
- CCS can also log any external device connection attempts.

This article explains how to:

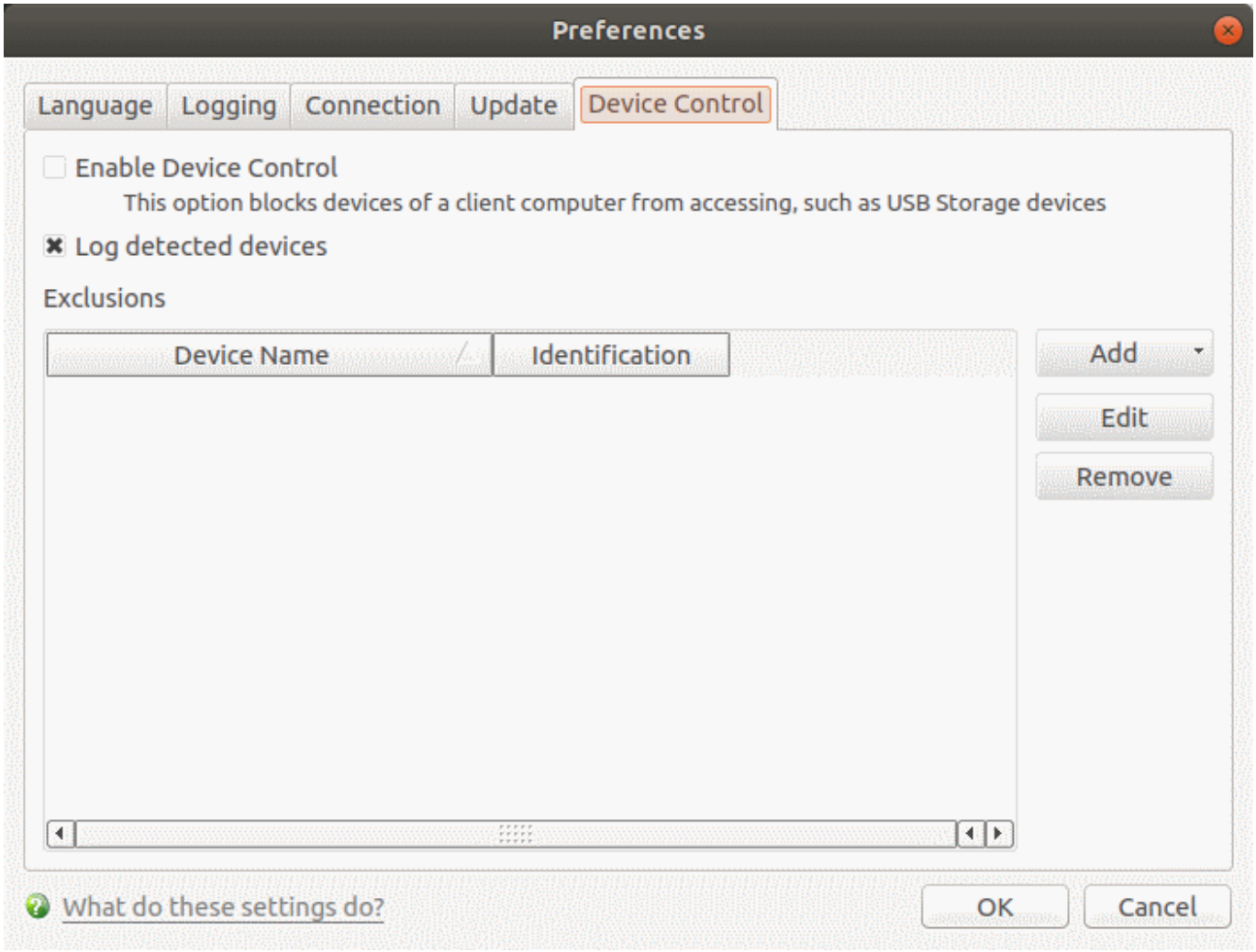
- Enable and configure external device control
- Add exclusions to device control
- View external connection attempt logs

Configure device control

- Login to the endpoint and open CCS. You can open CCS by clicking the dock icon:

- Click the ‘More’ tab then ‘Preferences’:

- Click the 'Device Control' tab:



- **Enable Device Control** - Prohibits access to external devices like USB cards and storage drives. You can define exclusions to allow selected devices to connect. (***Default = Disabled***)
- **Log detected devices** – CCS will keep a record of all device connection / disconnection events, whether they are blocked or not.
    - You can view logs in the 'Log Viewer' module.
    - Click 'More' > 'View Antivirus Events' > 'More' > 'Device Control Events'
    - See View device connection logs later in this article if you want more help on this.
- **Exclusions** - Add exceptions to device control. Devices you add here are allowed to connect to the endpoint, even if 'Device Control' is active. For example, if your company uses USB tokens to authenticate remote VPN connections, you should create exceptions for those tokens.
    - See the next section, 'Add exclusions to device control', for further help with this.

Add exclusions to device control

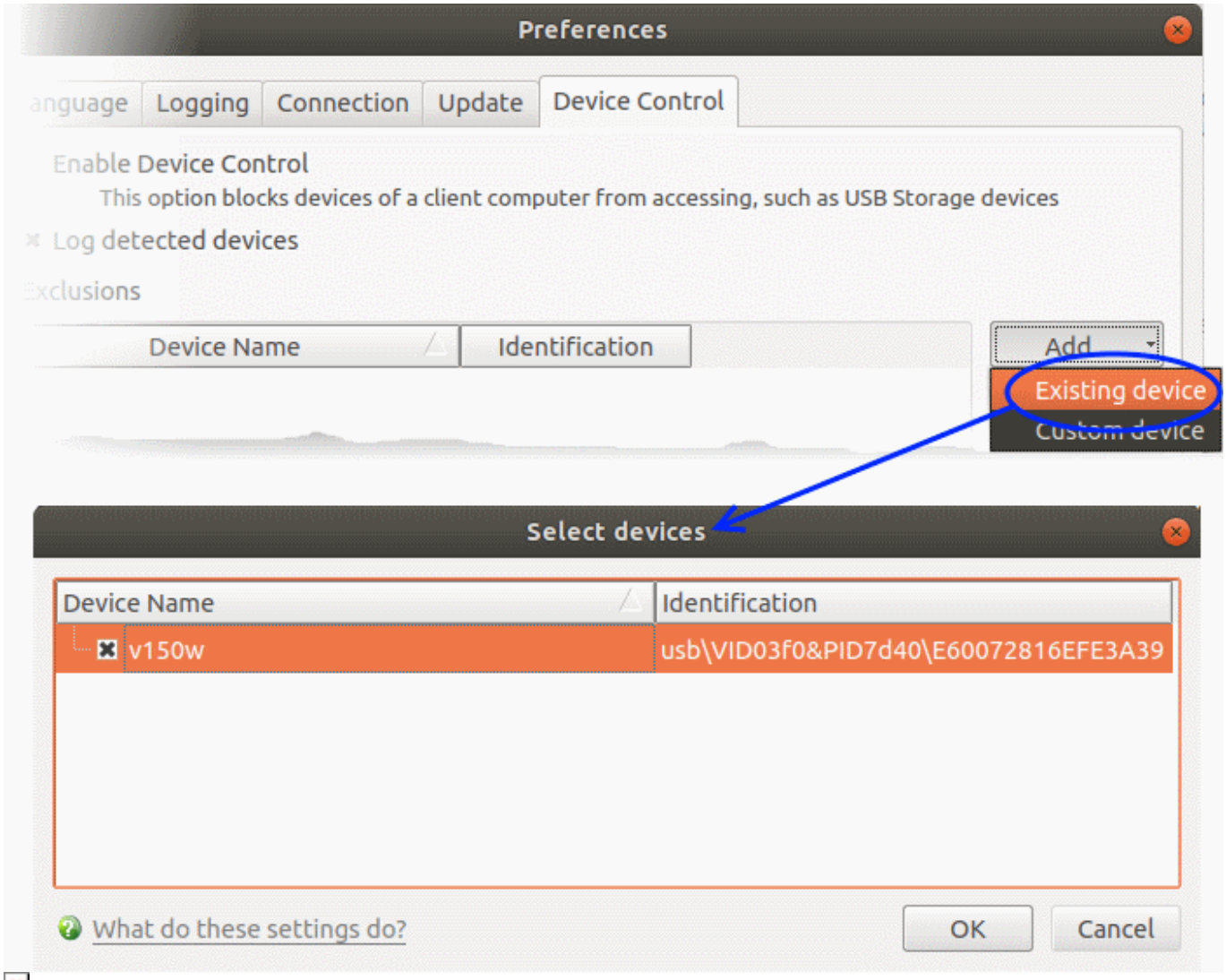
There are two ways you can specify exceptions:

- Select from currently connected devices
- Specify a custom device

Connect a device then create an exclusion for it

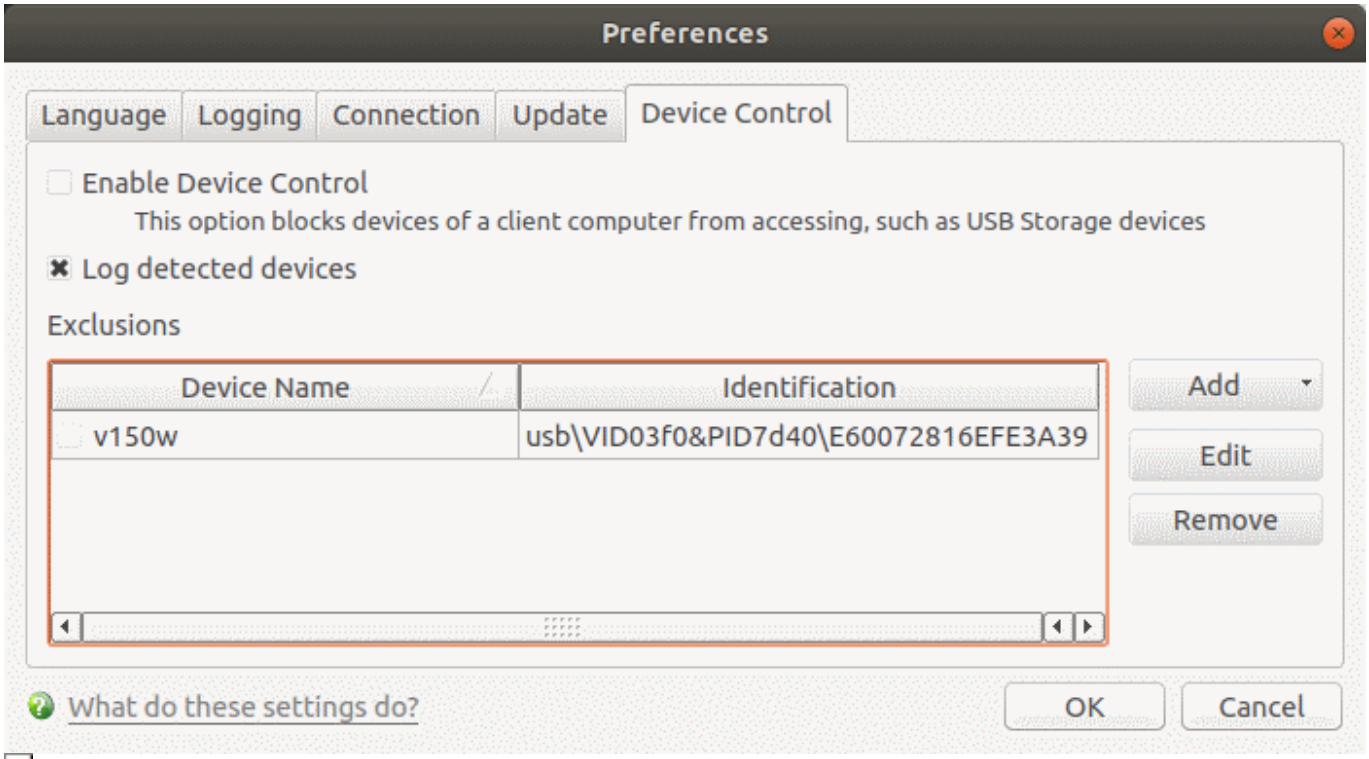
Note - You need to create your exceptions before enabling device control.

- Make sure the external device is connected to the computer
- Open Xcitium Client Security
- Click 'More' > 'Preferences' > 'Device Control':
- Click the 'Add' button then choose 'Existing Device' from the drop-down



The screen lists all devices that are currently connected to your computer.

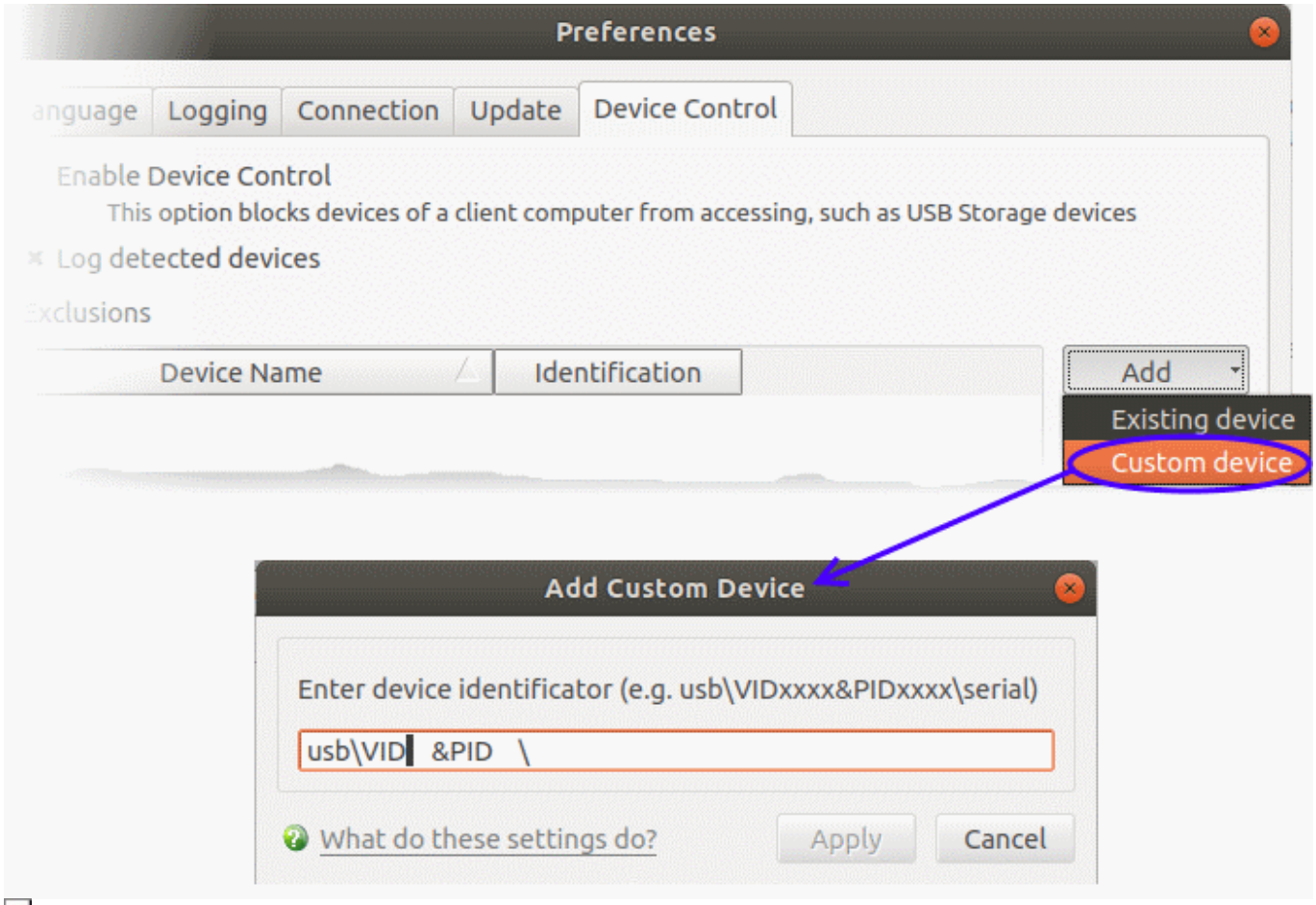
- Select the devices you want to add to exclusions and click 'OK'
- The device is added to the exclusions:



- Repeat the process to exclude more devices
- Click 'OK' in for your settings to take effect

Specify a custom device

- Open Xcitium Client Security
- Click 'More' > 'Preferences' > 'Device Control':
- Click the 'Add' button in the exclusions section then 'Custom Device':



- Enter the vendor identifier and product identifier in the respective areas. Example: VID0951&PID1643. You can use wildcard character to add a series of devices to exclusions. E.g. VID0951&PID16*
- Click 'Apply'

Click 'OK' in the 'Preferences' dialog for your settings to take effect

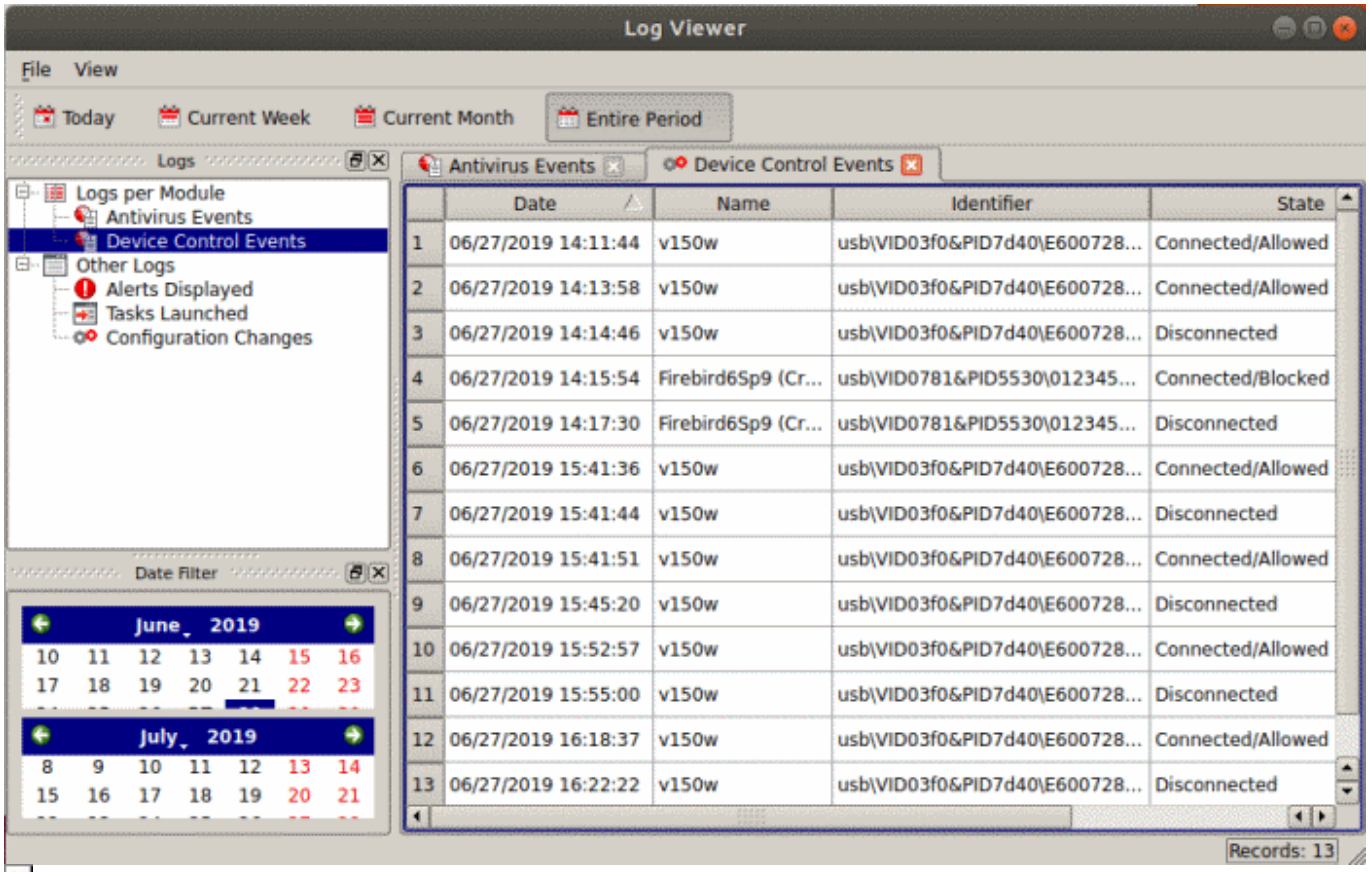
View device connection logs

CCS records external connection events if 'Log detected devices' is enabled in device control settings.

Each log shows the time of the connection / disconnection, the device connected, and whether the connection was allowed or blocked.

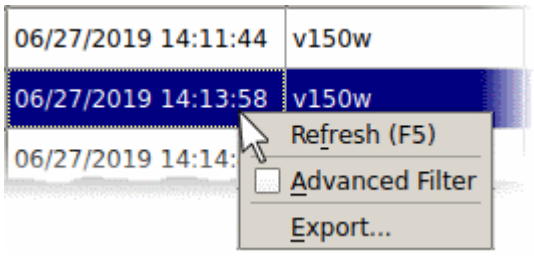
Open device control logs interface

- Open Xcitium Client Security
- Click 'More' > 'View Antivirus Events'
- Click the 'More' button to open the log viewer module
- Select 'Device Control Events' on the left:



- **Date** - Date and time of the connection event.
- **Name** - The label of the device.
- **Identifier** - The unique identification string of the device. The identifier Is a combination of the vendor identification number (VID) and the product identification number (PID).
- **State** - Whether the device was connected or disconnected, and whether the connection was allowed or blocked.

Right-click anywhere inside the log viewer to view further options:



- **Refresh** – Adds recently created logs to the list
- **Advanced Filter** - Filter device control events by various criteria, including name, identifier and state.
- **Export…** - Save the events list as an HTML file.