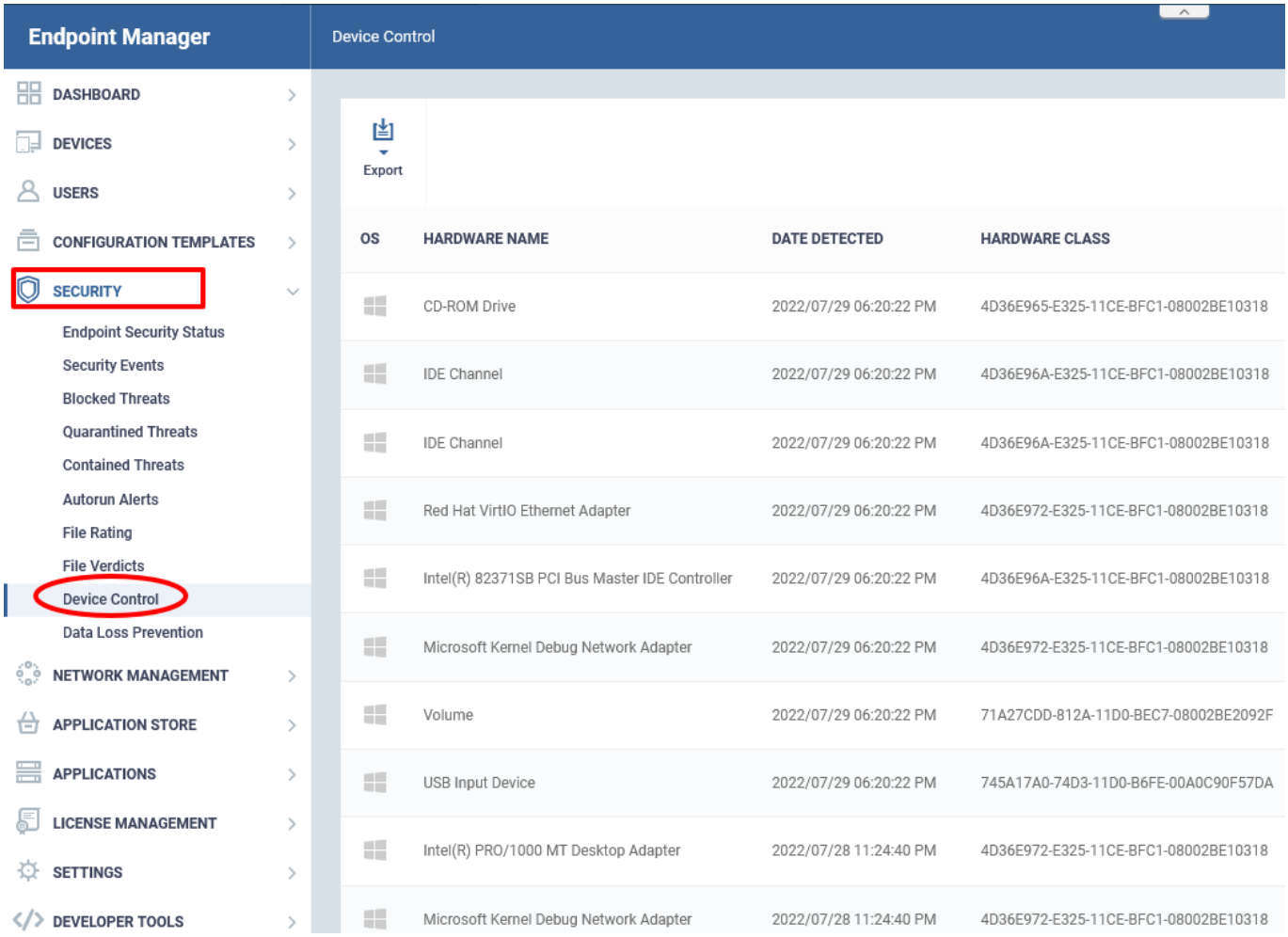
How to view connection attempts from external devices to your endpoints

Open Endpoint Manager > Click 'Security Sub-Systems' > 'Device Control'

- The device control area lets you view a history of connection attempts from external devices to your Windows endpoints. External devices include USB devices, Bluetooth devices, IDE ATA/ATAPI controllers and more.
- Endpoint Manager can also create a log when an external device attempts to connect to an endpoint.
- You can define which types of devices are blocked by adding an ‘External Device Control’ section to a profile. See this wiki for help to do this.
- This article explains the information and functionality of the device control section.

Open the device control area

- Log into Comodo One / Xcitium
- Click ‘Applications’ > ‘Endpoint Manager’
- Click 'Security Sub-Systems' > 'Device Control'
- Each row shows a moment in time when an external device connected or tried to connect, to an endpoint. Click the funnel icon on the right to filter the list.



Hardware Name - A broad description of the type of device that attempted to connect. For example, ‘Disk Drive’, or ‘CD Drive’

Date Detected - Date and time of the connection attempt

Hardware Class - The Global Unique Identifier (GUID) of the device. This code identifies the category, or ‘class’, of the external device. All devices of the same type will have the same GUID, even if they are different brands/models.

Hardware Path - The Device Instance Identifier. This is dynamically assigned to the device at the time it connects by the plug-n-play manager.

Host Device - The name of the Windows device to which the connection attempt was made. This column also shows the host's current connection status (connected or removed)

Status - Indicates whether the connection was allowed or blocked. This depends on the settings in the 'External Device Control' section of the endpoint’s profile.

The ‘Export’ button above the table lets you create a .csv file of all items in the list.

You can download the report from ‘Dashboard’ > ‘Reports’.

Further reading

How to view security events on Windows endpoints

How to manage programs running in containment on your endpoints

How to manage unknown & malicious files on your endpoints

How to run virus scans on devices from the security sub-systems menu