

# How to allow or block external devices connected to endpoints

Click 'Configuration Templates' > 'Profiles' > open a Windows profile > Open/Add 'External Device Control'

- The external device control section lets you block certain types of devices from connecting to managed endpoints.
- For example, you can block access to USB storage devices, Bluetooth devices, infrared devices, IDE ATA/ATAPI controllers.
- You can also create exceptions to allow specific devices to connect.

## Process in brief

- Log into Comodo One / Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'
- Open the Windows profile applied to your target devices
  - Open the 'External Devices Control' tab
- OR
- Click 'Add Profile Section' > 'External Devices Control' (if it hasn't yet been added)
- Click 'Edit'
- Select 'Enable device control'
  - Choose banned device types in the 'Blocked Device Classes' tab
  - Create exceptions for specific devices in the 'Exclusions' tab
- Click 'Save' for your settings to take effect

## Process in detail

- Log into Comodo One / Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'
  - Open the 'External Devices Control' tab

OR

- Click 'Add Profile Section' > 'External Devices Control' (if it hasn't yet been added)

<input type="checkbox"/>	OS	NAME	CREATED BY	CREATED
<input type="checkbox"/>	Windows	test123	dkrav	2022/07/27 04:49:41 PM
<input type="checkbox"/>	iOS	64451-Ios	dkrav	2022/07/13 12:14:33 PM
<input type="checkbox"/>	Android	64451-Android	dkrav	2022/07/13 12:13:54 PM
<input type="checkbox"/>	Linux	64451-Linux	dkrav	2022/07/12 09:43:35 PM
<input type="checkbox"/>	Windows	64451-Windows	dkrav	2022/07/12 09:43:14 PM
<input type="checkbox"/>	MacOs	64451-MacOs	dkrav	2022/07/12 09:42:40 PM
<input type="checkbox"/>	Windows	Windows - Containment Only Profile 7.1	admin	2022/07/06 12:42:21 AM
<input type="checkbox"/>	Windows	[cloned4fix] Windows - Containment Only Profile 7.1	admin	2022/06/29 04:29:55 PM
<input type="checkbox"/>	Windows	[imported] Containment Only	admin	2022/06/29 02:30:52 PM

The settings pane allows you to:????

- [Configure access control and logging settings](#)
- [Add blocked device types](#)
- [Specify exclusions](#)

### External device control settings

- **Enable devices control** – Activate or deactivate device access control
- **Log detected devices** – If enabled, any connection attempts by blocked device types are logged. You can view these logs at 'Security Sub-Systems' > 'Device Control'.
- **Show notifications when devices disables or enabled** – If enabled, an alert is shown to end-users when a device connection is blocked.

### Add blocked device types

- Click the 'Blocked Device Classes' tab
- Click 'Add'

Use this table to manage the list of device classes (e.g. "USB - Mass storage devices", "Optical devices"...

 Add  Delete

**DEVICE CLASS**

No results found.

### Add Device Class

<input type="checkbox"/>	DEVICE CLASS	CLASS ID
<input type="checkbox"/>	USB storage devices	8A63AD27-0CD7-4F43-B8E1-07AE6F236346
<input type="checkbox"/>	Human interface devices	745A17A0-74D3-11D0-B6FE-00A0C90F57DA
<input type="checkbox"/>	Floppy disks	4D36E980-E325-11CE-BFC1-08002BE10318
<input type="checkbox"/>	1394 FireWire devices	6BDD1FC1-810F-11D0-BEC7-08002BE2092F
<input type="checkbox"/>	IDE ATA/ATAPI controllers	4D36E96A-E325-11CE-BFC1-08002BE10318
<input type="checkbox"/>	Tape drives	6D807884-7D21-11CF-801C-08002BE10318
<input type="checkbox"/>	CD/DVD drives	4D36E965-E325-11CE-BFC1-08002BE10318
<input type="checkbox"/>	Printing devices	4D36E979-E325-11CE-BFC1-08002BE10318
<input type="checkbox"/>	PCMCIA	4D36E977-E325-11CE-BFC1-08002BE10318
<input type="checkbox"/>	Imaging devices	6BDD1FC6-810F-11D0-BEC7-08002BE2092F
<input type="checkbox"/>	Infrared devices	6BDD1FC5-810F-11D0-BEC7-08002BE2092F
<input type="checkbox"/>	Bluetooth devices	E0CBF06C-CD8B-4647-BB8A-263B43F0F974
<input type="checkbox"/>	SCSI	4D36E97B-E325-11CE-BFC1-08002BE10318
<input type="checkbox"/>	Modems	4D36E96D-E325-11CE-BFC1-08002BE10318
<input type="checkbox"/>	Smart card readers	50DD5230-BA8A-11D1-BF5D-0000F805F530
<input type="checkbox"/>	Ports	4D36E978-E325-11CE-BFC1-08002BE10318
<input type="checkbox"/>	Network adapters	4D36E972-E325-11CE-BFC1-08002BE10318
<input type="checkbox"/>	Biometric	53D29EF7-377C-4D14-864B-EB3A85769359
<input type="checkbox"/>	Disk drives	4D36E967-E325-11CE-BFC1-08002BE10318
<input type="checkbox"/>	Storage volumes	71A27CDD-812A-11D0-BEC7-08002BE2092F

« Prev | 1 | 2 | Next »

Results per page: 20

Displaying 1-20 of 21 results

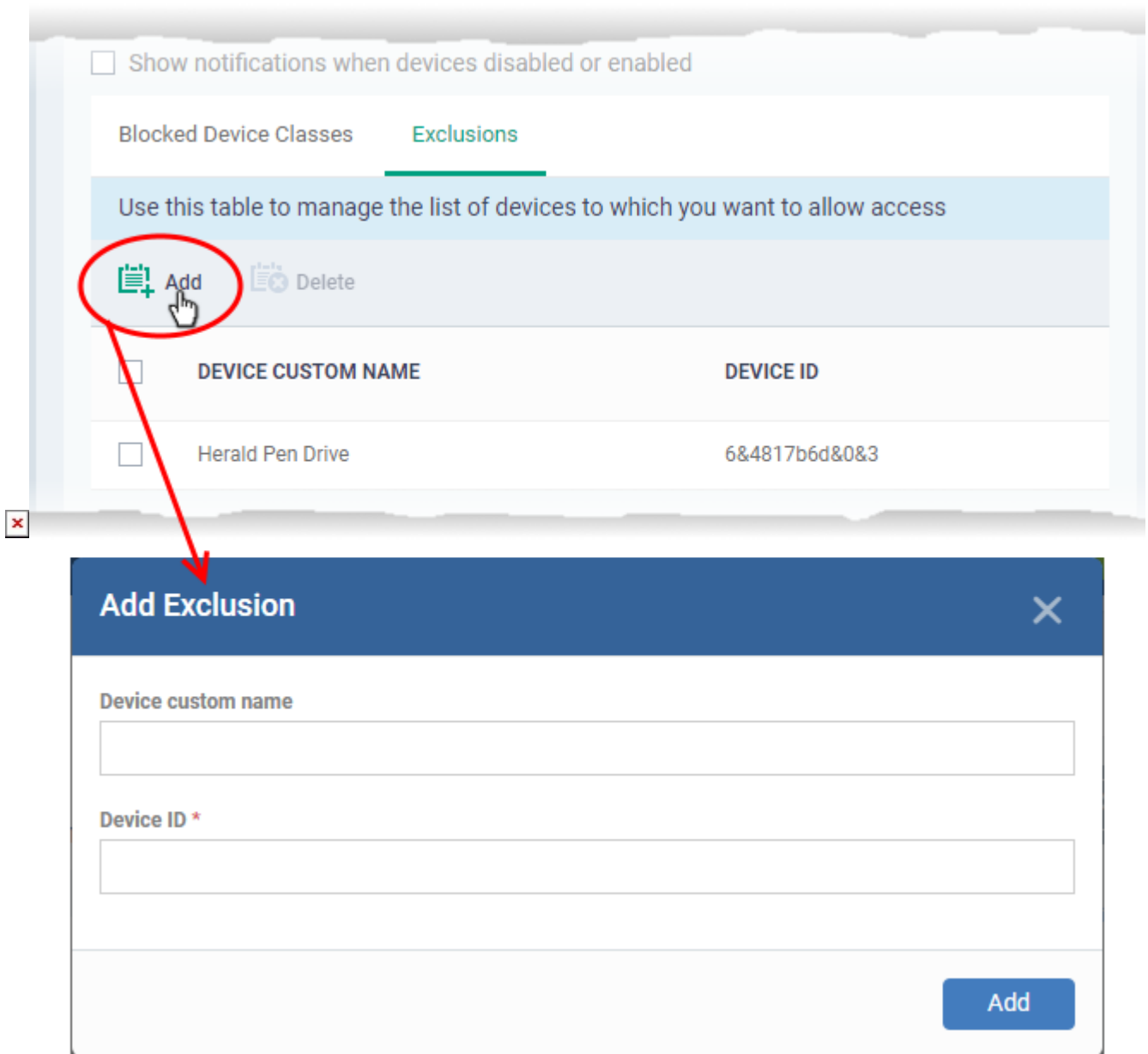
Ok

- Select the class of device you want to block then click 'Ok'.
- Repeat the process to add more device types.

### Exclusions

The exclusions tab lets you choose specific devices which are allowed to connect, even though you have banned the device class to which they belong. For example, you might ban the class 'USB Storage devices', but create an exception to allow your USB VPN tokens.

- Click the 'Exclusions' tab
- Click 'Add'



- Enter a label for the device in the 'Device Custom Name' field (optional)
- Enter the unique device identifier in the 'Device ID' field

- Example. If you want to block all USB storage devices apart from the type of SANDISK devices used by your company, you could specify a device exclusion ID of 'USBSTOR/DISK&VEN\_SANDISK/4C5310'.
- You can find the ID of any connected devices at 'Security Sub-systems' > 'Device Control' > 'Hardware Path' column.
- You can use a wildcard character '\*' if you want to cover a range of devices with similar IDs. For example, to include all USB storage devices whose IDs start with "4C5310", you could enter:

USBSTOR/DISK&VEN\_SANDISK/4C5310\*

- Click 'Add'

The device will be added to the exclusions list and allowed to connect to endpoints.

- Click 'Save' for your settings to take effect.