Reviewing Devices and Users.

Staying compliant with the requirements of Keeping Children Safe in Education

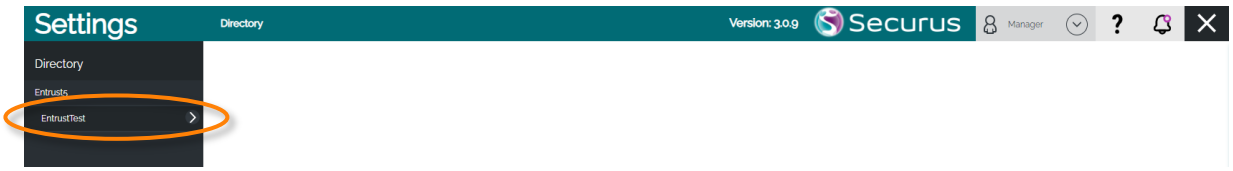
To reassure yourself that the monitoring is active on all the required devices in the school you can log in to the Securus console and see:

- the number and type of devices including the last time they were active.
- the names of the users that the system is monitoring including when they were last active.

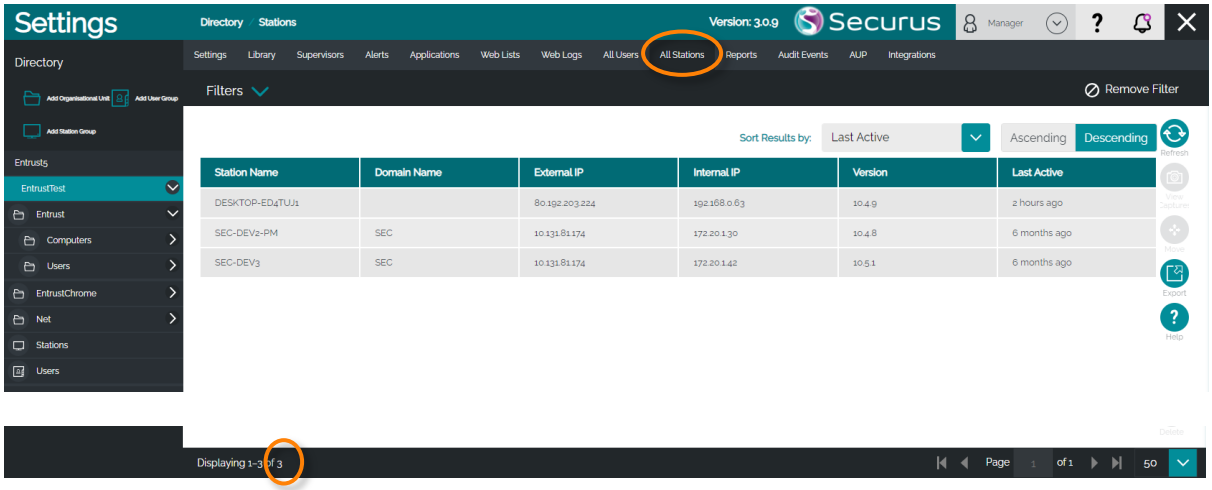
Identifying the number of devices being monitored

When logged in to the Securus console, click on the settings cog in the top right

Click on your school's name in the Directory on the left of the screen to show the settings menu's



Select 'All Stations' from the top menu.



This will give you a list of all the devices that have registered with the console and the last time they were active, along with a total number of devices at the bottom of the screen.

On the right is an option to export this list as a spreadsheet that can, for example, be sent to your technical support to check against your device audit to ensure that all the required devices are covered and identify any that might be missing.

Identifying specific types of devices

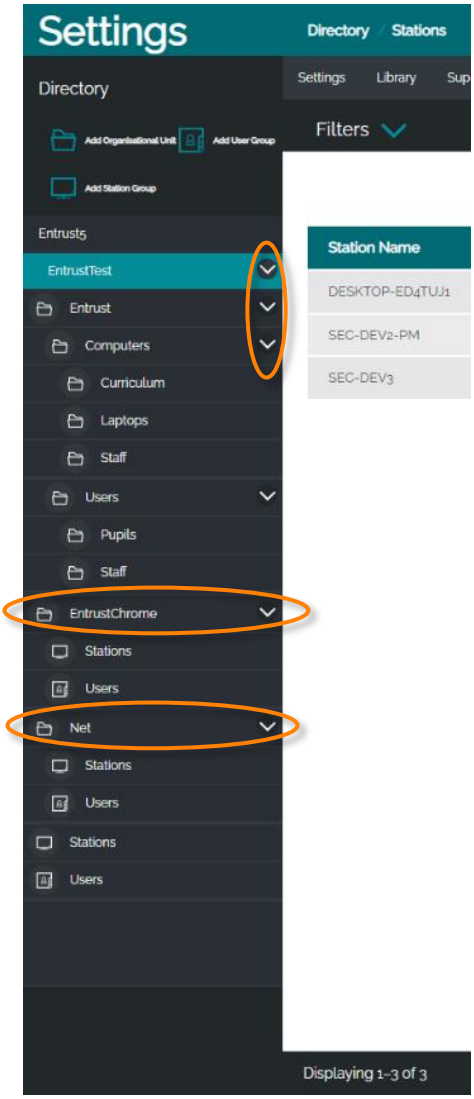
From the All Stations screen you can drill down to find the numbers of Chromebooks, iPads or Windows devices that are registered with the console.

Using the arrows in the directory, you can expand out the structure to see the different folders on the system.

To see the number of Chromebooks, click on the [schoolname]Chrome folder and the list on the right will update to show just the Chromebooks with the total at the bottom and the option to export the list.

To see the number of iPads (or other tablet devices), click on the Net folder and the list on the right will update to show just the Chromebooks with the total at the bottom and the option to export the list.
Note – if this folder is missing then the iPads have not been set up on the monitoring. The folder is automatically created when the first iPad registers.

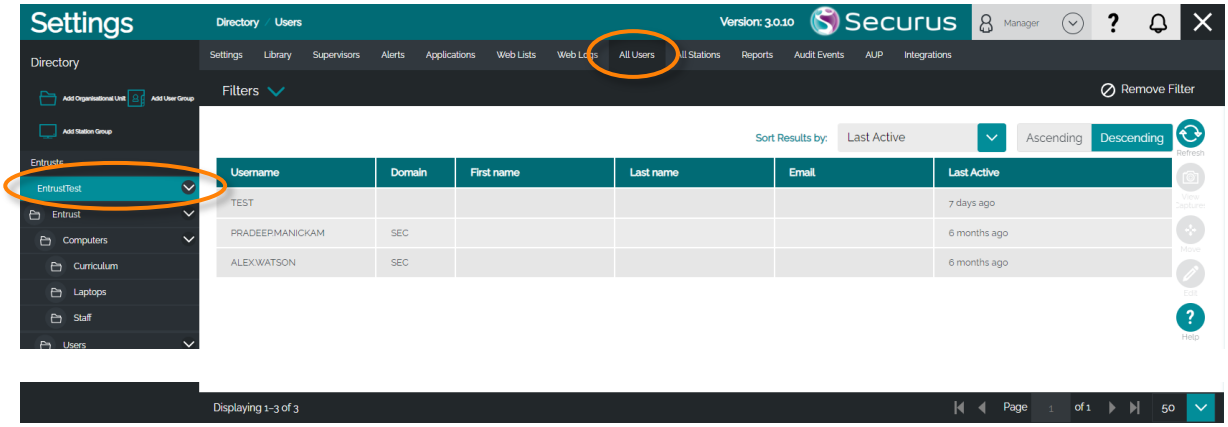
To see the number of Windows devices you will need to look through the Directory structure to find a Computers (or similar) folder. These folders come from your network structure and will have been set up by your technical team so will not appear the same as the screenshot. It might require some clicking on different folders to find the one you actually need! Depending how your network is set up you might be able to see folders for curriculum machines, Admin, staff or pupil machines or laptops as well.



If the top level All Stations list is empty, then the software has not been deployed to your devices and no monitoring is taking place. If any of the Chrome, Net or computers folders are empty then the software has not been deployed to those devices and they are not being monitored.

Identifying the number of users being monitored

When logged in to the Securus console settings, select ‘All Users’ from the top menu. Select the top-level school name from the left hand Directory menu.

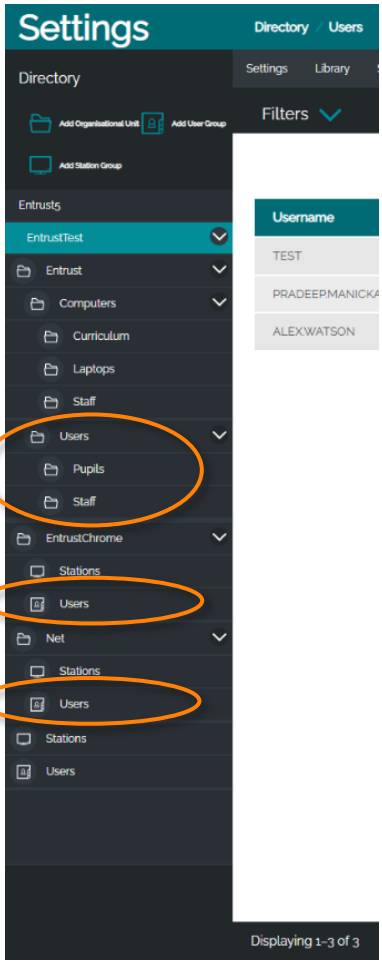


This will give you a list of all the users that have registered with the console and the last time they were active, along with a total number of users at the bottom of the screen.

This can be reviewed to check that the required users are covered and identify any that might be missing.

Identifying specific groups of users being monitored

As with the devices, it is possible to expand the Directory and look for the ‘Users’ groups within the structure. There will be Chrome Users and Net users within the relevant folders. Elsewhere in the structure you should be able to find Staff and Pupil/Student folders.
Clicking on any of these folders will update the list to show the users in that group allowing you to check if the numbers are accurate and identify any that are missing.



Net Users

If this group does not contain a recognisable username (it may be blank, contain IP addresses or hostnames) then this means that authentication has not been set up for the iPads.

Your technician can set up authentication so that the iPad users must log in when they go online meaning that any iPad captures will have their username against them making them easy to identify.