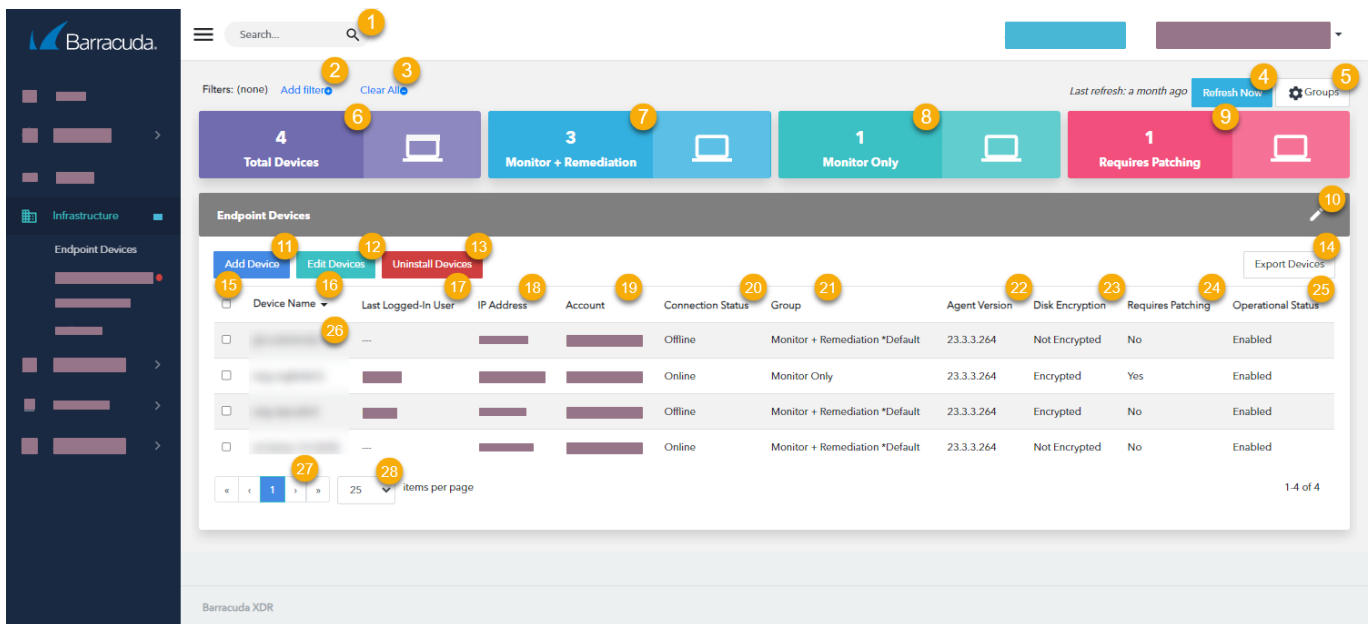


Working with the Endpoint Devices Page

<https://campus.barracuda.com/doc/102888005/>

The **Endpoint Devices** page gives you tools you need to protect your devices, including tools for protecting your device with the agent. To navigate to the page, click **Infrastructure > Endpoint Devices**. See the page graphic below.



The screenshot shows the Barracuda XDR interface. The left sidebar contains the 'Infrastructure' menu with 'Endpoint Devices' selected. The main content area features a search bar (1), filter controls (2, 3), and summary cards for 'Total Devices' (4), 'Monitor + Remediation' (7), 'Monitor Only' (8), and 'Requires Patching' (9). Below these is a table titled 'Endpoint Devices' with columns: Device Name (16), Last Logged-In User (17), IP Address (18), Account (19), Connection Status (20), Group (21), Agent Version (22), Disk Encryption (23), Requires Patching (24), and Operational Status (25). The table includes actions like 'Add Device' (11), 'Edit Devices' (12), and 'Uninstall Devices' (13). A table footer shows pagination (27) and items per page (28). Other UI elements include a 'Refresh Now' button (4), 'Export Devices' button (14), and a 'Groups' dropdown (5).

1. Type a search term to search.
2. Click to filter this page. See [Filtering the Endpoint Devices Page](#).
3. Click to clear all filters from this page.
4. Click to refresh the page.
5. Click to add or remove USB Blocking from one or more groups. See [Blocking and Unblocking USB Ports](#).
6. Displays the total devices in the account.
7. Displays the number of devices in the Monitor + Remediation group.
8. Displays the number of devices in the Monitor Only group.
9. Displays the number of devices that require patching.
10. Click to add a device to the account.
11. Add one or more selected devices to a group. See [Setting up Endpoint Security Groups](#).
12. Click to uninstall one or more selected devices.
13. Click to select the columns displayed in the table.
14. Click to export a .CSV file of the **Endpoint Devices** table. See [Exporting the Endpoint Devices Table](#).
15. Select or clear a check box in this column to select devices.
16. Displays the device name. Click the arrow to sort the table by this column.
17. Displays the name of the user who logged in to the device most recently.

18. Displays the device's IP address.
19. Displays the account the device belongs to.
20. Displays the device's connection status.
21. Displays the group the device belongs to.
22. Displays the version of the agent on the device.
23. Displays whether the disks on the device are encrypted or not.
24. Displays if the agent has detected that an application requires a patch due to a CVE.
25. Displays the status of the agent on the device.
26. Click a device row to do any of the following:
 - Snooze endpoint protection on the device for 1 hour, 6 hours, or 24 hours. See [Snoozing and Unsnoozing Protection on Devices](#)
 - Add the device to a group.
 - Uninstall the device. See [Uninstalling Endpoint Protection from a Device](#).
 - Set a log degradation threshold of 1 day, 3 weeks, 6 months, or 1 year. See [Setting a Threshold for Log Degradation](#)
27. Click the forward or back arrows to navigate the pages.
28. Click to select the number of devices displayed per page.

Figures

1. Page with numbers1.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.