Cisco Identity Devices

Devices

Devices are often an important piece of the Identity puzzle. Knowing what devices exist in your organization can help answer questions to aid in investigations, like what users are associated with certain devices and which users are actually using that device, as well as in posture clean ups to reduce device related risks such as removing stale or abandoned devices, or blocking devices that run operating systems that are no longer supported. It can also help with policy making decisions such as understanding which devices have been used to access certain tools or resources in your organization so that you can determine the blast radius of a policy configuration change; however, finding the device data needed to answer these types questions can prove challenging for many organizations.

Similar to the Users page or the User 360 Devices tab, the **Devices** page in Cisco Identity enables you to visualize all the mobile, desktop, laptop, and other types of devices discovered via your connected identity sources, such as Entra ID, Duo, or Okta, as well as Mobile Device Managers (MDMs) like as Jamf, to give you cross-platform insight across your organization.

The Devices page is different from the User 360 Devices tab, however, because the Devices page will aggregate the same device seen across multiple sources into one device “record” and will also display devices that are not associated with any users in your environment.

This aggregated view gives organizations visibility into their device landscape so they can quickly and easily find concerns, filter on certain issues or drill into particular use cases to answer their questions and enable them to take corrective action on the devices within their environment.

This article provides information about the different data and functionality that exists in the Devices page such as:

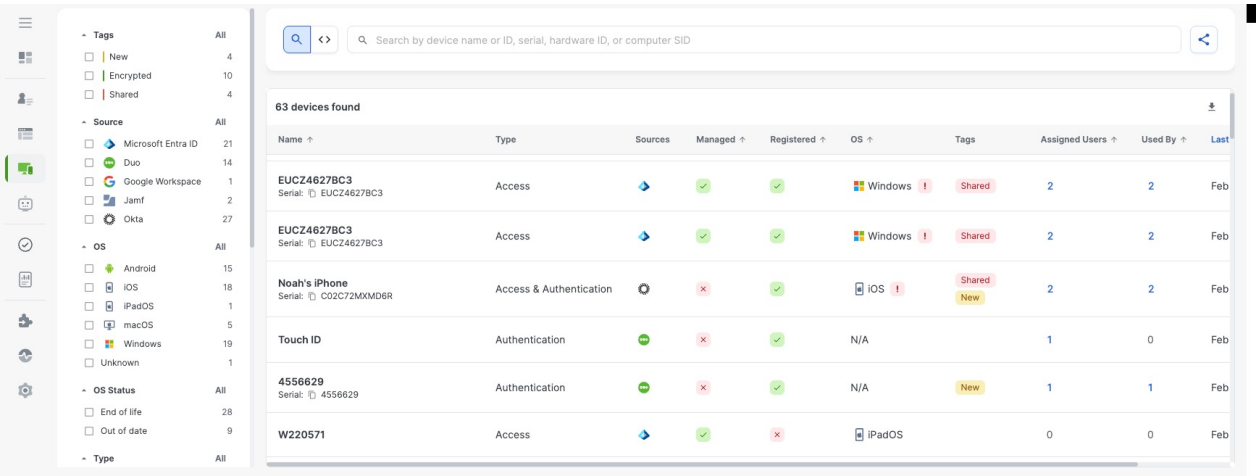
- Definitions of the elements in the table
- Diving deeper into a device
- Filtering
- General functionality such as searching, exporting results, sharing, etc

Devices table elements

By default, devices are sorted by date of access (most recent first). There are no default filters applied on the Devices page.

The total number of Devices in the table is displayed above the column headers of the table itself.

Example:



The table below explains the meaning of the columns that appear in the table:

Column	Meaning
Name	Name and serial number (if available) of the device
Type	**Access:** Devices, such as a desktop computer, that can be used to connect or gain entry to your organization's systems. **Authentication**: Devices, such as a mobile phones, that can be used as a multi-factor authentication (MFA) method to validate a user's identity when signing in to a system. Typically these devices must be enrolled as a MFA device for a specific Identity Provider, such as Duo. **Access & Authentication:** Devices that can be used for both, such as a laptop (access) with a built-in fingerprint scanner that is enrolled for MFA (authentication).
Sources	Identity sources associated with a given device. If the same device can be associated across more than one source using a common, strong device identifier, such as a serial number, the devices are aggregated into one device record.
Managed	Managed devices are those are have been enrolled in an organization's centralized management system such as an MDM, Unified Endpoint Management (UEM) or IT Service Management tool. These devices are typically company owned and provided to its users with pre-installed MDM software. Devices are “managed” to meet compliance requirements or enforce security policies. Typically, the user logs in to a managed device before being allowed to access network resources. Example: A Duo trusted endpoint or a device managed by Microsoft Intune. A filled indicator = Device is managed by an organization, as reported by identity source or

	MDM. An empty indicator = Device is not managed by an organization, as reported by from identity source or MDM
Registered	Sometimes referred to as joined, a device can be registered with your organization by logging in to the device and joining the work network. (The user can optionally download and install MDM software like Microsoft Intune.) A registered device might be either provided by the organization or it might be a personal device. A filled indicator = Device is registered. An empty indicator = Device is not registered.
OS	Name of the operating system. A warning icon  will be displayed next to the operating system type to indicate if the device is either out of date or end of life. A red background indicates the OS is `end of life`; a yellow background indicates `out of date`. Hover the mouse pointer over the icon to see the device's current OS version and status.
Tags	Cisco Identity-assigned tags, including: Shared: More than one user logged into the device, which may indicate credential sharing. The Assigned Users column displays the number of users who share the device. New: Device has been recently detected and has not been seen before. Encrypted: Device is encrypted.

Assigned Users	Number of users allocated to that device via the IdP or MDM. Devices that are **not** assigned to a user will still appear in the table. Hover over the number to view the user names (if the number is non-zero) or select the number to drill into the Users page, pre-filtered on the associated user(s)
Used By	Number of users with recent events using that device. Devices do **not** need to have recent usage to appear in the table. If the number is non-zero, hover over it to view the user names or select the number to view the Users page, pre-filtered on the associated users.
Last Seen (UTC)	Universal time code-formatted date and time the device was last seen by the identity source.

Diving deeper into a device

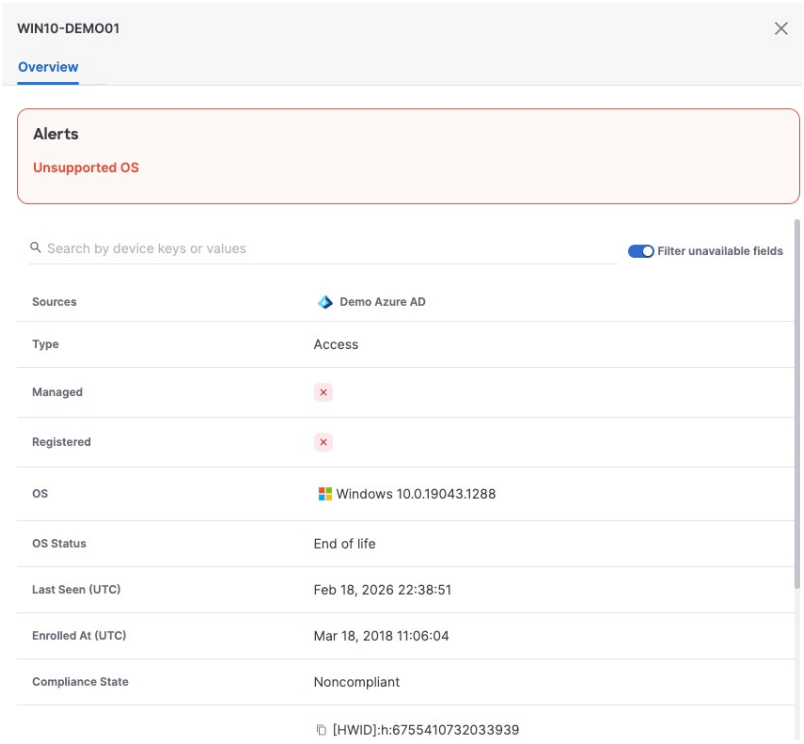
Clicking the name of a device, or anywhere in the row that is not a link, opens a slide panel from the right side of the page that contains more detailed information about the device.

The available attribute fields for each device will vary depending on the source reporting the device, based on what information that source is able to share with Cisco Identity.

You can use the search field to quickly locate certain attribute types or values on this page.

To close the slide panel, select the **X** in the top right corner, or select anywhere outside the slide panel.

Example:



Filters

You can filter the Devices table by a number of attributes, enabling you to search for devices based on the parameters that are important to you or easily identify devices that may need to be remediated or removed.

There are two types of filters that can be used on the Devices table - basic filters, which can be found to the left of the Devices table and Advanced Query mode, which can be enabled via the **\<>** button next to the search bar above the Devices table. Check out our documentation on how to use Advanced Query Mode to learn more about this functionality.

Devices page general actions

The Devices page includes several features that can be found elsewhere in the platform:

Search

Use the search bar to search based on device name, serial name, tags, sources and so on. When searching, you do not need to provide an exact value. Entering a piece of the word will return results.

If you have searched on a particular parameter, the search criteria is retained as you navigate between different tabs within the platform.

To clear the search bar, click the **X** on the right side.

Sort columns

Sort columns within the table by selecting the column header you'd like to sort by. Select once to sort in ascending order, select again to sort in descending order.

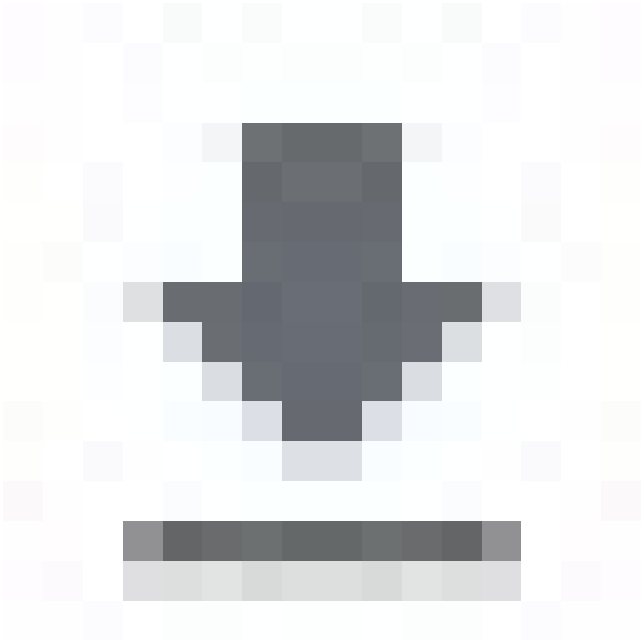
Multi-column sorting is not currently supported.

Download results

Download tabular data from the table to a CSV using the **Download** icon button found the right side above the table column headers.

If there are no results in the table, the CSV export contains only headers and no user data.

Note: The CSV download has a limit of 2,000 rows. If you need to download more than 2,000 rows, click the download button and follow the prompts to get the export sent using a download link.



Share results

The **Share** button (on the right side of the Search bar) copies a link to this page, with the applied filters and selected columns, that can be easily pasted, bookmarked or shared with anyone who has the appropriate access to your Cisco Identity tenant.

