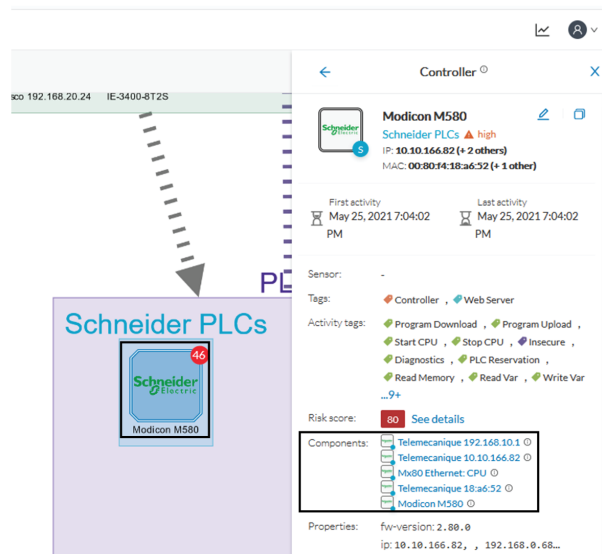# Device

# Device

The concept of device has been developed to show the network from a physical point of view (in Cisco Cyber Vision versions older than 4.0.0 only components and aggregated components were used). A device represents in Cisco Cyber Vision a physical machine of the industrial network such as a switch, an engineering station, a controller, a PC, a server, etc. Thus, devices simplify data presentation, especially in the map, and enhance performances; because a single device will be shown in place of multiple components. Besides, it complies with a logic of management and inventory, which focuses on users' needs.

In the GUI, a device is shown as an icon in a double border, either the manufacturer icon (if detected), or a more specific icon (for instance for a known PLC model), or even a default cogwheel if no icons is available in Cisco Cyber Vision database yet.



Technically, a device is an aggregation of components that have been brought together because they have similar properties. In fact, components can share same characteristics such as same IP address, same MAC address, same Netbios name, etc. In addition, tags and properties which are found in protocols are associated to define the type of device. Aggregation of components into a device and definition of the device type are based on a large set of rules with priorities that can be more or less complex.

*As you click on a device -on the left, a Schneider controller-, a right side panel opens showing its components:*

Devices can have a red counter badge which display the number of vulnerabilities detected. For more information, refer to Vulnerabilities.

*The list of a Rockwell Controller device's components (technical sheet > Basics > Components):*

## 5 Components

| Component | First activity | Last activity | IP | MAC | Tags | Vulnerab |
|---|---|---|---|---|---|---|
| 1756-EN2T/D ⓘ | May 25, 2021 7:02:23 PM | May 25, 2021 7:02:23 PM | 192.168.20.22 | 4c:71:0d:72:8c:57 | Rockwell Automation | 11 |
| 1756-RM2/A REDUNDANCY MODULE (Port1-Link01) ⓘ | May 25, 2021 7:02:23 PM | May 25, 2021 7:02:23 PM | 192.168.20.22 | 4c:71:0d:72:8c:57 | Rockwell Automation | 0 |
| 1756-EN2T/D (Port1-Link02) ⓘ | May 25, 2021 7:02:23 PM | May 25, 2021 7:02:23 PM | 192.168.20.22 | 4c:71:0d:72:8c:57 | Rockwell Automation | 11 |
| 1756-EN2TR/C (Port1-Link03) ⓘ | May 25, 2021 7:02:23 PM | May 25, 2021 7:02:23 PM | 192.168.20.22 | 4c:71:0d:72:8c:57 | Rockwell Automation | 11 |
| L71RED_CPU_NAME \| 1756-L71/B LOGIX5571 ⓘ | May 25, 2021 7:02:23 PM | May 25, 2021 7:02:23 PM | 192.168.20.22 | 4c:71:0d:72:8c:57 | Controller , Rockwell Automation | 2 |

All these device's components have in common activity time, IPs, MACs, and tags. The Controller tag -which is a level 2 device tag, also considered as top priority in aggregation rules to define device type- detected on one of the components is applied at the device level and define the device type as Controller. The Rockwell Automation tag is a system tag which together with other properties is detected as the brand of the device.

To know which types of device Cisco Cyber Vision is capable of detecting, take a look at the device tags classified per level in the Cisco Cyber Vision application.