



## Risk score

---

- [Risk score, on page 1](#)

## Risk score

### Risk Score Definition

A risk score is an indicator of the good health and criticality level of a device. The scale is from 0 to 100 with a color code indicating the level of risk.

Score	Color	Risk level
From 0 to 39	Green	Low
From 40 to 69	Orange	Medium
From 70 to 100	Red	High

Risk scores apply to the following:

- Filter criteria
- Device list
- Device technical sheet
- Device risk score widget (Home page)
- Preset highlight widget (Home page)

### Risk Score Use

Risk score helps you easily identifying which devices are the most critical within the overall network. It provides limited and simple information on the cybersecurity of the monitored system. It is a first step in security management by showing values and providing solutions to reduce them. The goal: minimize values and keep risk scores as low as possible.

Proposed solutions are:

- Patch a device to reduce the surface of attack

- Remove vulnerabilities
- Update firmware
- Remove unsafe protocols whenever possible (e.g., FTP, TFTP, Telnet),
- Install a firewall
- Limit communications with the outside by removing external IPs

Cyber Vision allows you to define the importance of the devices in your system by grouping them and setting an industrial impact. This function increases or decreases the risk score, allowing you to focus on the most critical devices.

All these actions reduce the risk score which affect its variables, i.e., the impact and the likelihood of a risk. For example, removing unsafe protocols will affect the likelihood of the risk, but patching a device will act on the impact of the risk.

Risk score presents an opportunity to update usage and maintenance habits. However, it is NOT intended to replace a security audit.

In addition, risk scores are used in Cisco Cyber Vision to sort out information by ordering and filtering criteria in lists and to create presets.

### **Risk Score Computation**

Risk score is computed as follows:

$$\text{Risk} = \text{Impact} \times \text{Likelihood}$$

Impact is the device “criticality”, that is, what is its impact on the network? Does the device control a small, non-significant part of the network, or does it control a large, critical part of the network? Impact depends on:

- Device tags: Some device types are more critical. Each device type (or device tag) or device tag category is assigned an industrial impact score by Cisco Cyber Vision. For example, the device is a simple IO device that controls a limited portion of the system or it is a Scada that controls the entire factory. These will not have the same impact if they are compromised.
- You effect the device impact by moving it into a group and setting the group's industrial impact (from very low to very high).

Likelihood is the probability of this device being compromised Likelihood of risk depends on the following:

- Device activities and the activity tags. Some protocols are less secure than others. For example, Telnet is less secure than ssh.
- The exposure of the device communicating with an external subnet.
- Device vulnerabilities, taking into account their CVSS scoring.

For detailed information about a risk, see **Details** tab inside the technical sheet.

### **How to take action:**

1. In the top menu banner, click **Explore > All data > Dashboard > Device List**.

Explore / All data / Device list

Last 1 year (Jun 3, 2020 5:50:32 PM – Jun 3, 2021 5:50:32 PM) Refresh

14 Devices and 32 other components New data Export to CSV

1 / 46 Devices selected Select all devices Clear selection

Device	Group	First activity	Last activity	IP	MAC	Risk score
<input checked="" type="checkbox"/> Modicon M580	Schneider PLCs	May 25, 2021 7:04:02 PM	May 25, 2021 7:04:02 PM	192.168.0.68 (+ 2 others)	00:80:f4:18:a6:52 (+ 1 other)	80
<input type="checkbox"/> L71RED_CPU_NAME   1756-L71/B LOGIX5571	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.21	4c:71:0d:72:8c:57	75
<input type="checkbox"/> L81ES   1756-L81ES/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.25	4c:71:0d:72:8c:57	75
<input type="checkbox"/> L306_V01   5069-L306ERS2/B	Rockwell PLCs	May 25, 2021 7:02:23 PM	May 25, 2021 7:02:23 PM	192.168.20.23	4c:71:0d:72:8c:57	75

2. In the **Device List**, **Risk score** column, click the **Sort arrow** to get the highest risk scores.
3. Click a device in the list. Its right side panel opens.
4. In **Risk score**, click the **See details** link.

Controller

**Modicon M580**  
Schneider PLCs **high**  
IP: 10.10.166.82 (+ 2 others)  
MAC: 00:80:f4:18:a6:52 (+ 1 other)

First activity: May 25, 2021 7:04:02 PM  
Last activity: May 25, 2021 7:04:02 PM

Sensor: -

Tags: Controller, Web Server

Activity tags: Program Download, Program Upload, Start CPU, Stop CPU, Insecure, Diagnostics, PLC Reservation, Read Memory, Read Var, Write Var, ...9+

**Risk score: 80** [See details](#)

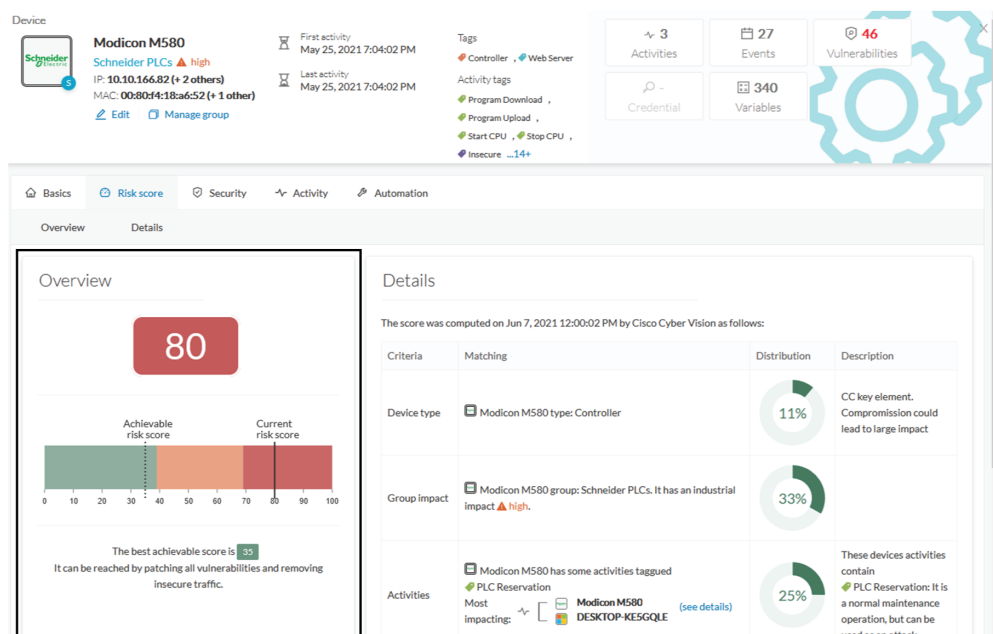
Components: Telemecanique 192.168.10.1, Telemecanique 10.10.166.82, Mx80 Ethernet: CPU, Telemecanique 18:a6:52, Modicon M580

Properties: fw-version: 2.88.0  
in: 192.168.10.1, 10.10.166.82

The technical sheet opens.

In the **Overview** tab, the **Current** risk score and the **Achievable** risk score display.

The achievable risk score is the best score you can reach if you patch all vulnerabilities on the device and remove all potential insecure network activities. The score cannot be zero because devices have intrinsic risks coming from their device type and, if applicable, their group industrial impact.



The **Details** tab shows further information about the different risks impacting the device, the percentage of the risk they represent within a total risk score, and the solutions to reduce or even eliminate them.

**Device type** and **Group impact** affect the risk impact variable. **Activities** and **Vulnerabilities** affect the risk likelihood.

Details

The score was computed on Jun 7, 2021 12:00:02 PM by Cisco Cyber Vision as follows:

Criteria	Matching	Distribution	Description
1 Device type	Modicon M580 type: Controller	11%	CC key element. Compromise could lead to large impact
2 Group impact	Modicon M580 group: Schneider PLCs. It has an industrial impact <span style="color: red;">▲</span> high.	33%	
3 Activities	Modicon M580 has some activities tagged PLC Reservation Most impacting:  Modicon M580 DESKTOP-KE5GQLE (see details)	25%	These devices activities contain PLC Reservation: It is a normal maintenance operation, but can be used as an attack
4 Vulnerabilities	Modicon M580 most impacting vulnerability is Multiple vulnerabilities in modicon controllers	31%	<b>Multiple vulnerabilities in modicon controllers</b> CVE-2018-7842 CVSS score: 9.8 A CWE-290: Authentication Bypass by Spoofing vulnerability exists which could cause an elevation of <a href="#">...show more</a> <a href="#">See details</a>

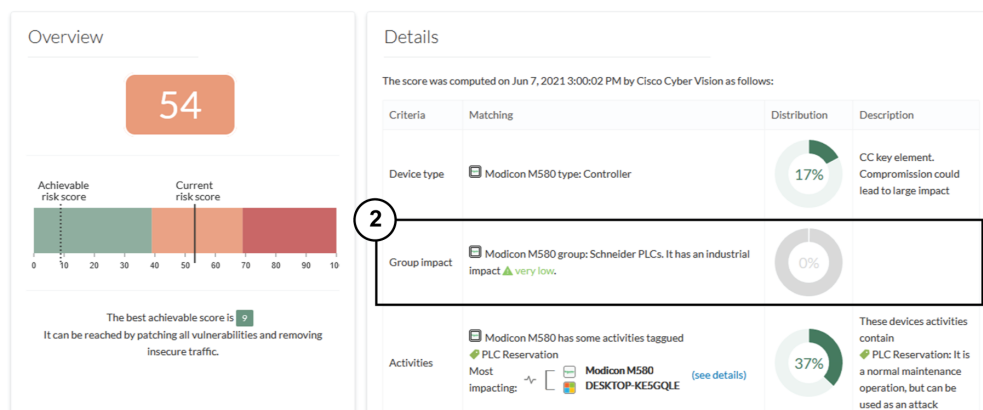
This page shows the last time the risk score was computed by Cisco Cyber Vision. Risk score computation occurs once an hour. To force immediate computation, use the following command on the Center shell prompt:

```
sbs-device-engine
```

Below is an example of the information retrieved during the last computation.

- **Device type:** Each device type corresponds to a [device tag](#) detected by Cisco Cyber Vision. No action is required at the device type level because each device tag is assigned a risk score by default.
- **Group impact:** Action is possible if the device belongs to a group. Decrease the impact by lowering the industrial impact of the group that the device belongs to.

For example, if you set the group industrial impact to very low (previously high), the overall risk score decreases from 80 to 54.



**Note** The new industrial impact will factor into the next risk score computation (once an hour).

- **Activities:** The most impactful activity tag displays. To lower the risk, remove all potential insecure network activities.
- **Vulnerabilities:** Click the **See details** link for more information about how to patch the vulnerabilities and so reduce the device risk score.

**Details**

The score was computed on Jun 7, 2021 12:00:02 PM by Cisco Cyber Vision as follows:

Criteria	Matching
Device type	Modicon M580 type: Controller
Group impact	Modicon M580 group: Schneider PLCs. It has an industrial impact <span style="color: red;">▲</span> high.
Activities	Modicon M580 has some activities tagged Most impacting: PLC Reservation, Modicon M580 DESKTOP-KE5GQLE (see details)
Vulnerabilities	Modicon M580 most impacting vulnerability is Multiple vulnerabilities in modicon controllers

**4 Vulnerability**

**9.8** CVSS score v3  
Multiple vulnerabilities in modicon controllers

Identifier: CVE-2018-7842

Description: A CWE-290: Authentication Bypass by Spoofing vulnerability exists which could cause an elevation of privilege by conducting a brute force attack on Mo... [show more](#)

Solution: The vulnerabilities described in this document are linked to weaknesses in the management of Modbus protocol. Products with no fix available can be mi... [show more](#)

Published on: May 14, 2019

Links: [Schneider](#)

By taking these actions, the risk score should decrease considerably.