



# Reports

- [Reports, on page 1](#)
- [Legacy Reports, on page 5](#)

## Reports

Security posture reports allow you to export industrial network data from the traffic captured and processed by Cisco Cyber Vision.

That way, you can show off striking information like sensitive entrance points, acknowledged vulnerabilities for status reports, etc.

You must install the reports extension to be able to use this page. You can do so by importing the reports extension file through the Admin Extension page in Cisco Cyber Vision. The extension file is available on [cisco.com](https://cisco.com).

The screenshot shows the Cisco Cyber Vision interface. On the left is a dark navigation sidebar with the Cisco logo and 'CYBER VISION' text, and menu items: Explore, Reports, Events, Monitor, Search, and Admin. The main content area has a 'Reports' dropdown menu and a user profile icon. Below this, there are tabs for 'Reports' and 'Legacy Reports'. A message box states: 'Please install the Reports extension to create new reports using the customized Reporting workflow. Installation steps can be found in the guide [here](#). Remember to log out and log back in after the installation is complete.' Below the message, it says '0 Report' and '+ Create and run a Report'. There is a pagination control showing '1' of '20 / page'. A table with the following columns is shown: Name, Preset, Created by, Last Modified, Status, Last Run, and Actions. The table is empty, with a 'No data' message and a folder icon at the bottom.

Security posture reports allow you to create reports from a [preset](#), that is a set of data, present by default in Cisco Cyber Vision, or a custom one.

Reports are exportable in docx and pdf formats.

You can customize the report by adding a logo, such as the company's one. By default, the report will be generated with Cisco's logo.

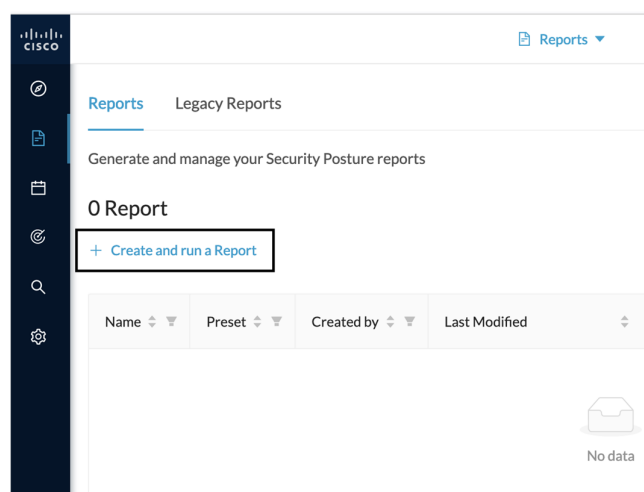
The table of content menu allows you to set which content will appear in the report.

## Create a report

### Procedure

#### Step 1

Click **Create and run a report**.



#### Step 2

Give the report a name and optionally add a description.

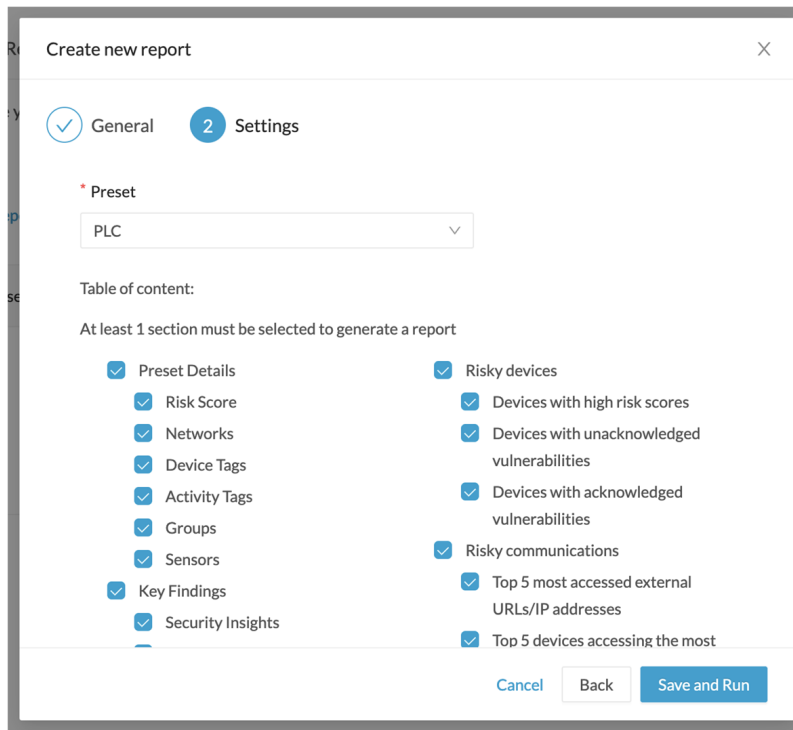
**Step 3** Optionally, add a logo. It will appear on the report.

**Step 4** Select the format(s) you want the report to be generated to.

**Step 5** Click Next.

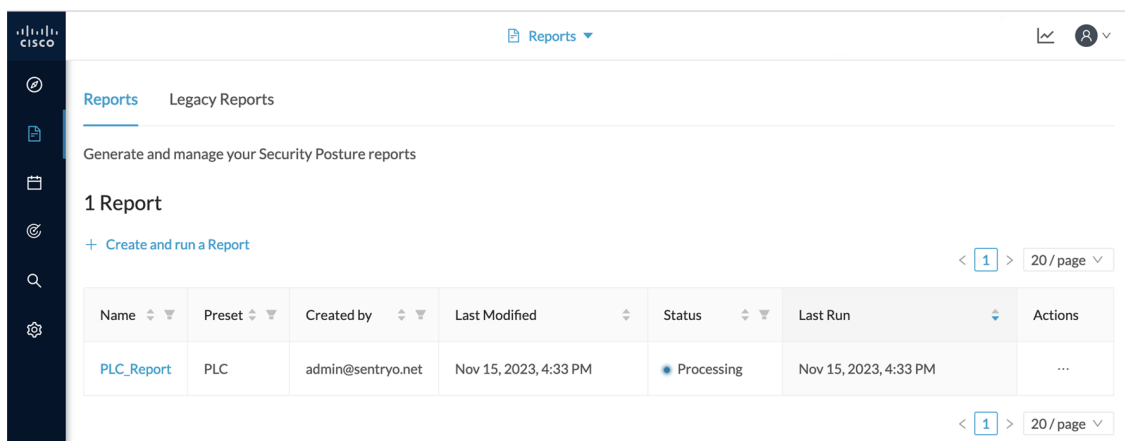
**Step 6** Select a preset from the dropdown menu.

**Step 7** Under table of content, select the content you want to appear in the report.

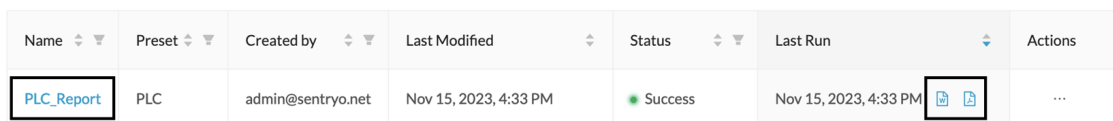


**Step 8** Click **Save and run**.

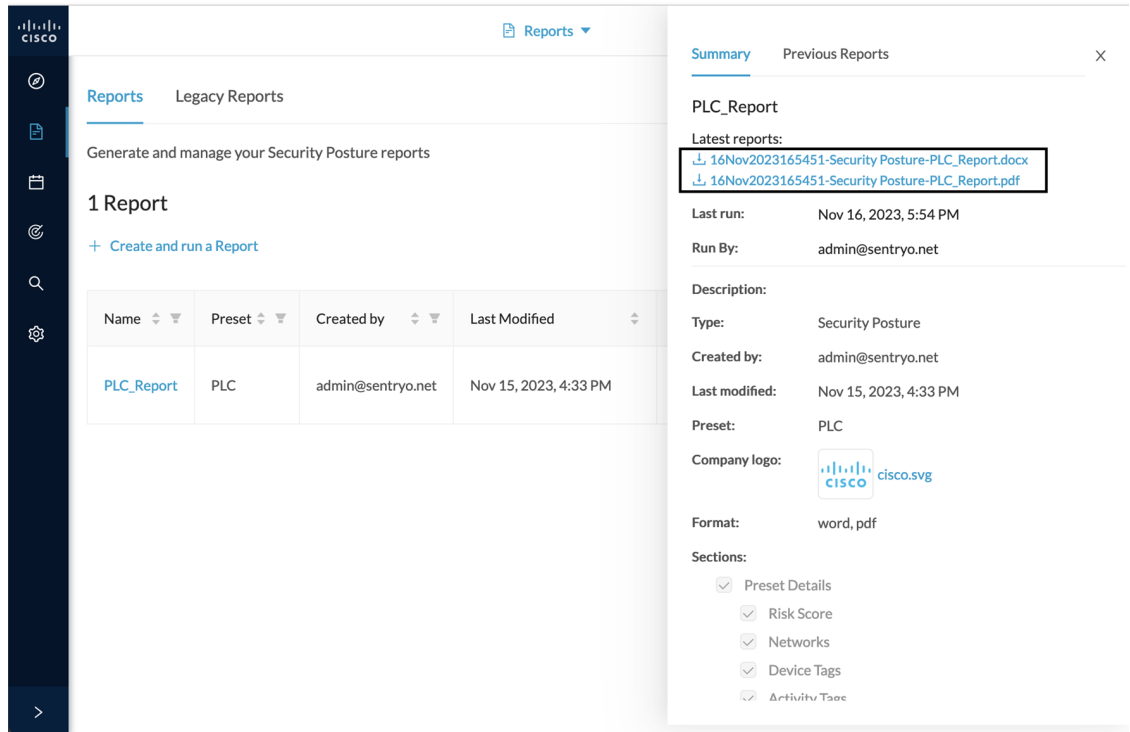
The new report appears in the list with the status Processing. It should eventually turn to Success after a few moment once the report is generated.



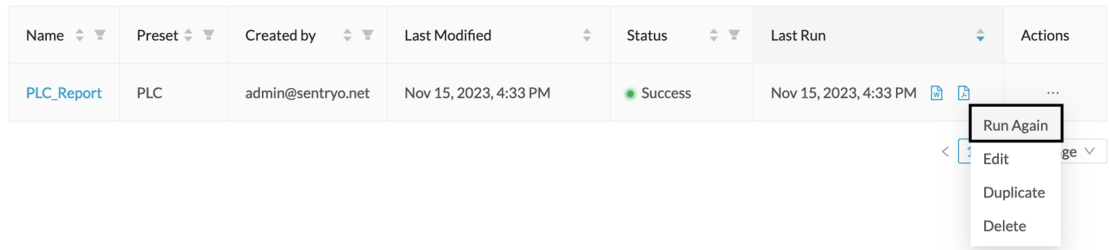
**Step 9** To download the report, click the name of the report in the list to open its right side panel or the format button(s).



**Step 10** On the right side panel, click the links to download the latest reports. You will find older ones under the Previous Reports menu.

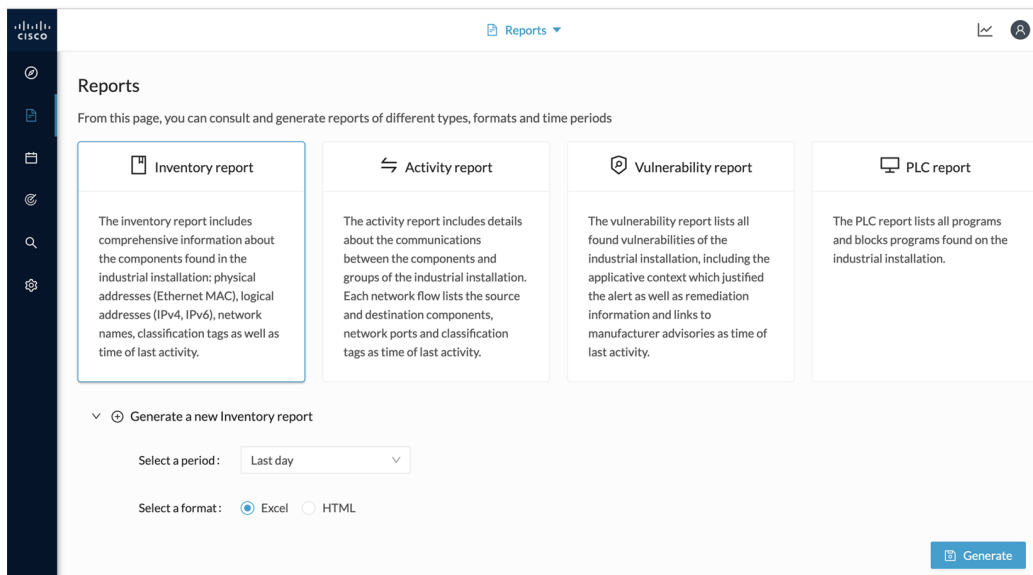


**Step 11** To generate a new report click **Run Again** under Actions.



## Legacy Reports

Legacy reports are exportable files which improve your visibility of valuable information about your industrial network. Information are collected and categorized according to different perspectives which are components, flows, vulnerabilities and PLCs. Reports can be generated for a time period you define into spreadsheets (XLSX) or printable (HTML that you can export to PDF).



Below is the description of the four types of reports available:

- The **inventory report** lists and details all components of your industrial network. They are sorted by group. For each component different information is given like the component name, when it was active for the first and the last time and tags that qualify its activity. If available, you will also find technical details such as its MAC and IP addresses, hardware and firmware versions, the serial number and extra properties.
- The **activity report** lists and details all communications exchanged between the components of your industrial network. They are sorted by group and by direction (inner, incoming and outgoing communications regarding a group). Information provided includes the protocol, which source and destination ports have been used and tags that qualify its activity.
- The **vulnerability report** lists all components detected as vulnerable and gives further details about vulnerabilities. Vulnerabilities are based on the Knowledge DB provided by Cisco. So, the more you keep the Knowledge DB up to date, the better you will be notified about new known vulnerabilities. The report contains information about the vulnerability, its impact level, its CVSS (Common Vulnerability Scoring System) and solutions. A vulnerability is often about outdated software parts. It is strongly recommended to fix outdated states as soon as possible. Links to manufacturers' websites are provided for this purpose.
- The **PLC report** lists all PLCs in your industrial network. For each PLC, the report lists and details properties, events, programs, program blocks and variable accesses, if there are any.

All reports generated are displayed in the History section from which you can rename, download and delete reports.

