



Reports

- [Reports, on page 1](#)

Reports

Reports are exportable files which improve your visibility of valuable information about your industrial network. Information is 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).

The screenshot displays the Cisco Industrial Network Security (INS) Reports interface. At the top, there is a navigation bar with the Cisco logo and several icons. The main content area is titled "SELECT A REPORT" and contains four report options, each with an icon and a brief description:

- Inventory report**: The inventory report includes comprehensive information about the components found in the industrial installation: physical addresses (Ethernet MAC), logical addresses (IPv4, IPv6), network names, classification tags as well as time of last activity.
- Activity report**: The activity report includes details about the communications between the components and groups of the industrial installation. Each network flow lists the source and destination components, network ports and classification tags as time of last activity.
- Vulnerability report**: The vulnerability report lists all found vulnerabilities of the industrial installation, including the applicative context which justified the alert as well as remediation information and links to manufacturer advisories as time of last activity.
- PLC report**: The PLC report lists all programs and blocks programs found on the industrial installation.

Below the report selection area, the "Activity report" configuration section is visible. It includes a "Select a period" dropdown menu set to "Last Day", a "Select a format" section with radio buttons for "Excel" (selected) and "HTML", and a "GENERATE ACTIVITY REPORT" button.

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.

