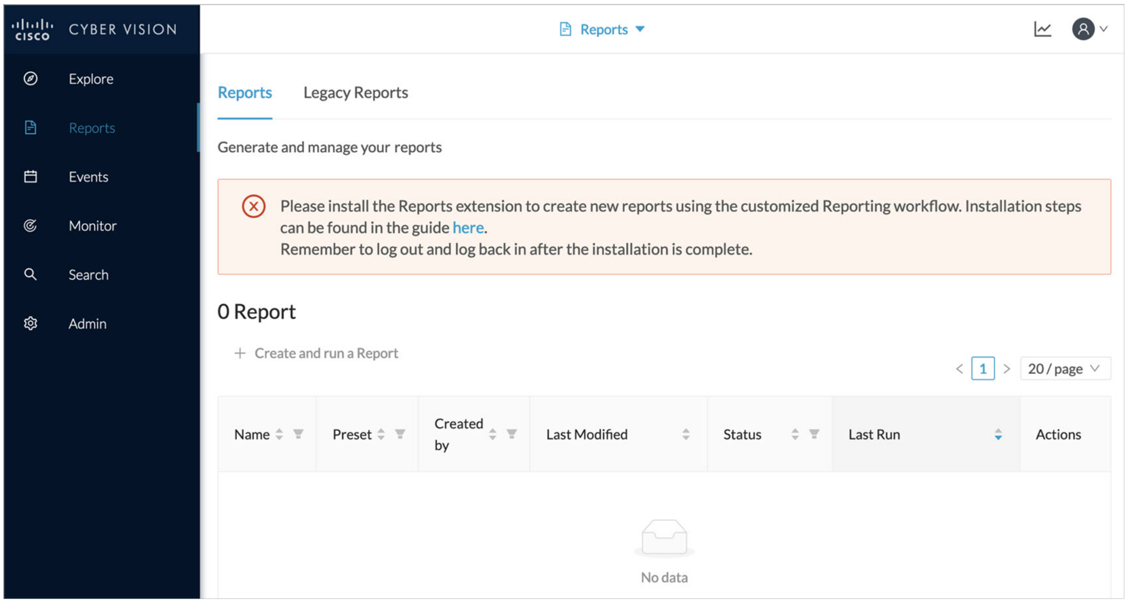
Reports

Reports

Security posture reports allow you to export industrial network data from the traffic captured and processed by Cisco Cyber Vision. You can uncover striking information like sensitive entrance points, acknowledged vulnerabilities for status reports, etc. To access **Reports**, click **Reports** from the black banner.

You must install the **Reports extension** to use this page. Click **Admin** > **Extension** > **Import a new extension file**. The extension file is available on cisco.com.



Generate and manage your reports

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.

0 Report

Name	Preset	Created by	Last Modified	Status	Last Run	Actions

No data

Security posture reports allow you to create reports from a preset, (default data) in Cisco Cyber Vision, or a custom one.

Reports extensions include .docx and .pdf formats.

You can customize the report by adding a logo, such as your company's logo. By default, the report shows Cisco's logo.

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

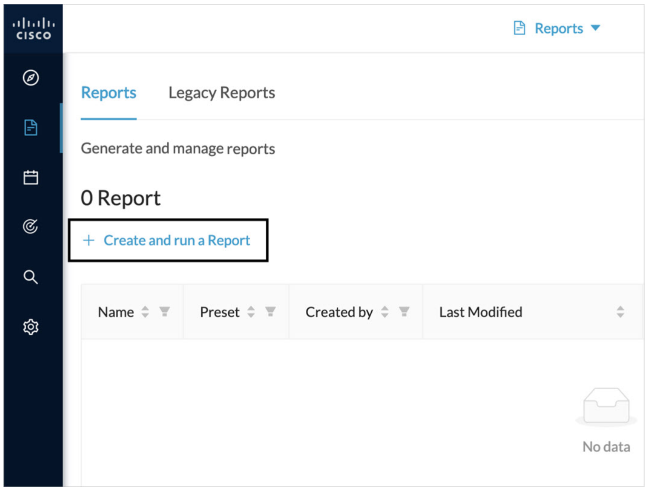
Create a report

Note **Cyber Vision Reports Management** extension and **Cyber Vision Version** must be the same to generate the report.

Procedure

Step 1 From left pane, click **Reports**

Step 2 Click **Create and run a Report**.



Reports

Reports

Legacy Reports

Generate and manage reports

0 Report

+ Create and run a Report

Name	Preset	Created by	Last Modified

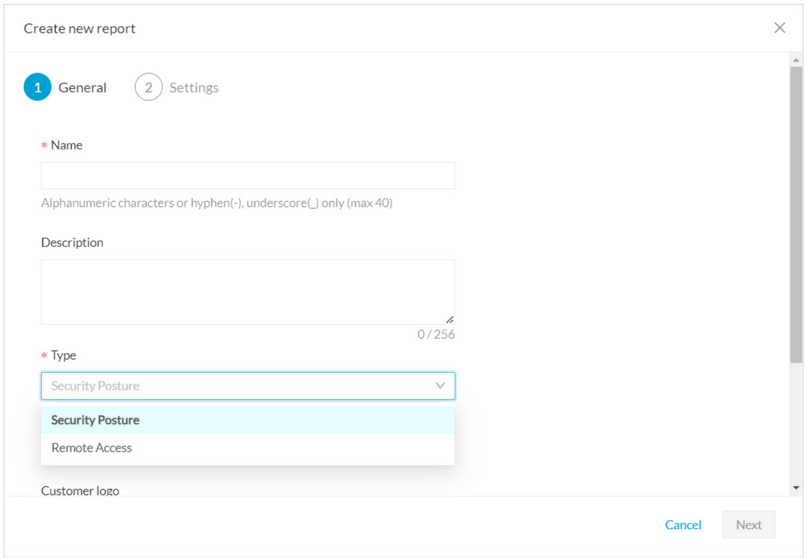
No data

Step 3 Type a **Name**. Optionally, add a **Description**.

Step 4 Select the report type from the dropdown list. Report types are as follows:

- **Security Posture:**This report is an automated summary that captures all the vulnerabilities, risky acivities, and security events found on the devices in the selected preset by Cisco Cyber Vision.
- **Remote Access:**This report is an automated summary that captures a list of all Remote Access Gateways and the Remote Access related activities found on the devices in the selected preset by Cisco Cyber Vision.

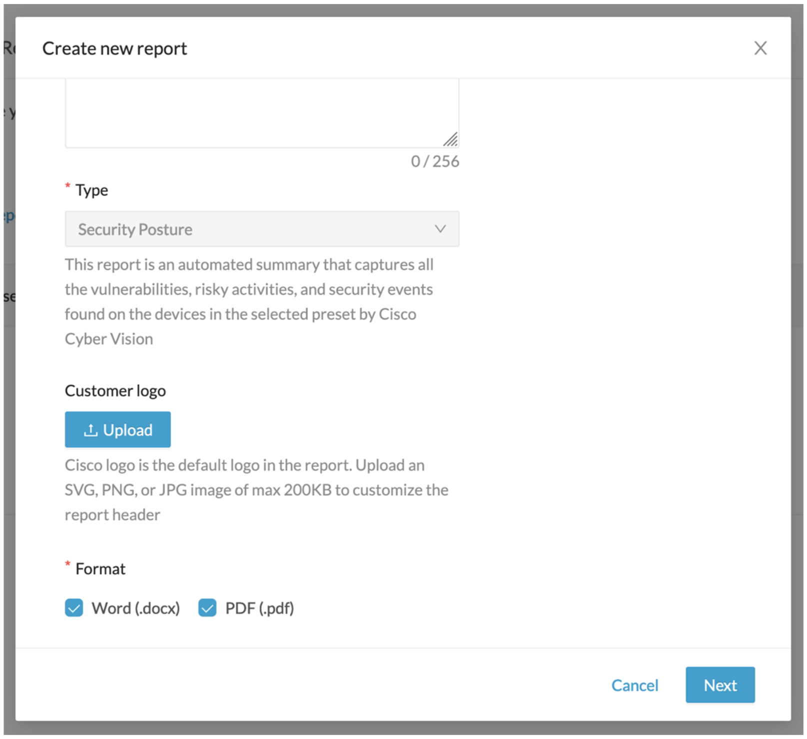
Note Only users with report access and correct permission can create reports. Users with read-only access can download reports.



Alphanumeric characters or hyphen(-), underscore(_) only (max 40)

Step 5 Optionally, add a **Customer logo**. It will appear on the report.

Step 6 Select the **Format**(s) you want.



This report is an automated summary that captures all the vulnerabilities, risky activities, and security events found on the devices in the selected preset by Cisco Cyber Vision

Cisco logo is the default logo in the report. Upload an SVG, PNG, or JPG image of max 200KB to customize the report header

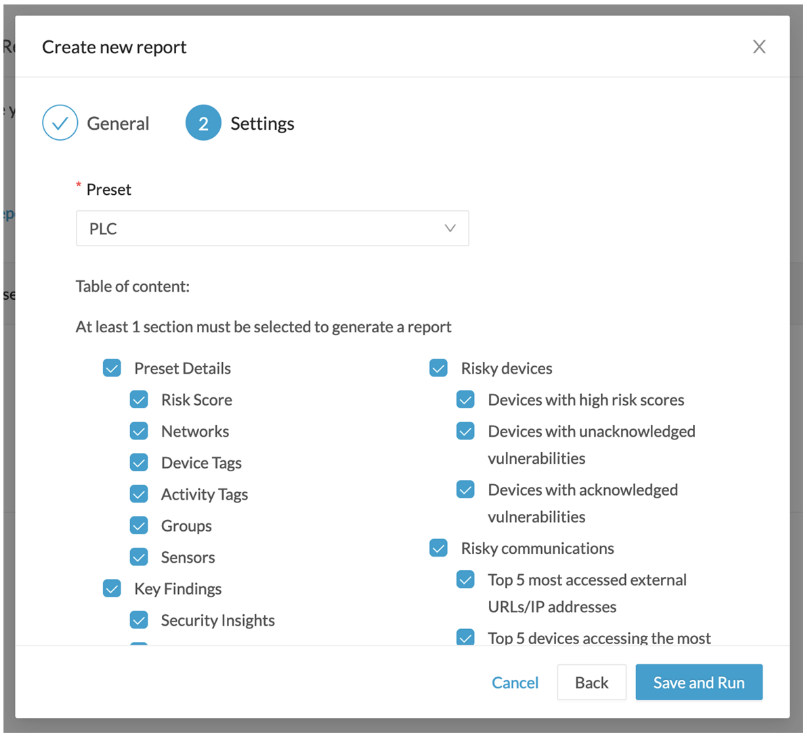
☑ Word (.docx) ☑ PDF (.pdf)

Step 7 Click **Next**.

Step 8 Select a **Preset** from the drop-down menu.

Step 9 In **Table of content**, select the content (sections and sub-sections) you want to appear in the report.

Note Content (sections and sub-sections) will vary depending on the type of report selected.



Create new report

✓ General 2 Settings

* Preset

PLC

Table of content:

At least 1 section must be selected to generate a report

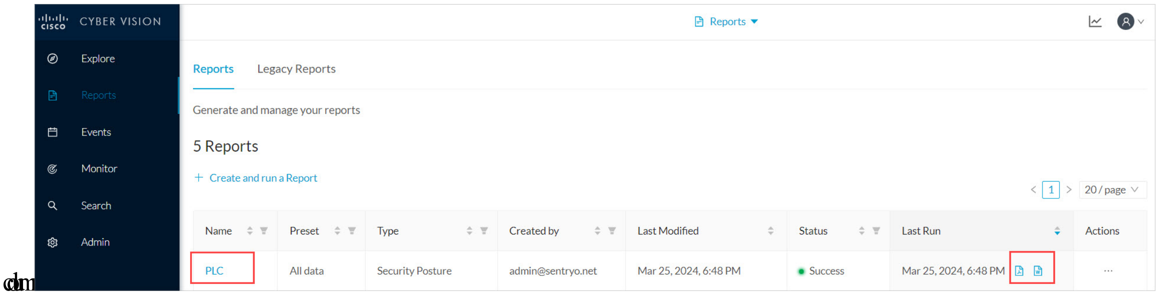
- ☑ Preset Details
  - ☑ Risk Score
  - ☑ Networks
  - ☑ Device Tags
  - ☑ Activity Tags
  - ☑ Groups
  - ☑ Sensors
- ☑ Key Findings
  - ☑ Security Insights
- ☑ Risky devices
  - ☑ Devices with high risk scores
  - ☑ Devices with unacknowledged vulnerabilities
  - ☑ Devices with acknowledged vulnerabilities
- ☑ Risky communications
  - ☑ Top 5 most accessed external URLs/IP addresses
  - ☑ Top 5 devices accessing the most

Step 10 Click **Save and Run**.

The new report appears in the list with the **Status: Processing**. When done, **Success** appears.

Step 11 To download the report, click the name of the report in the list to open its **Detail** panel. Or, use the format icon(s) in the **Last Run**

dm



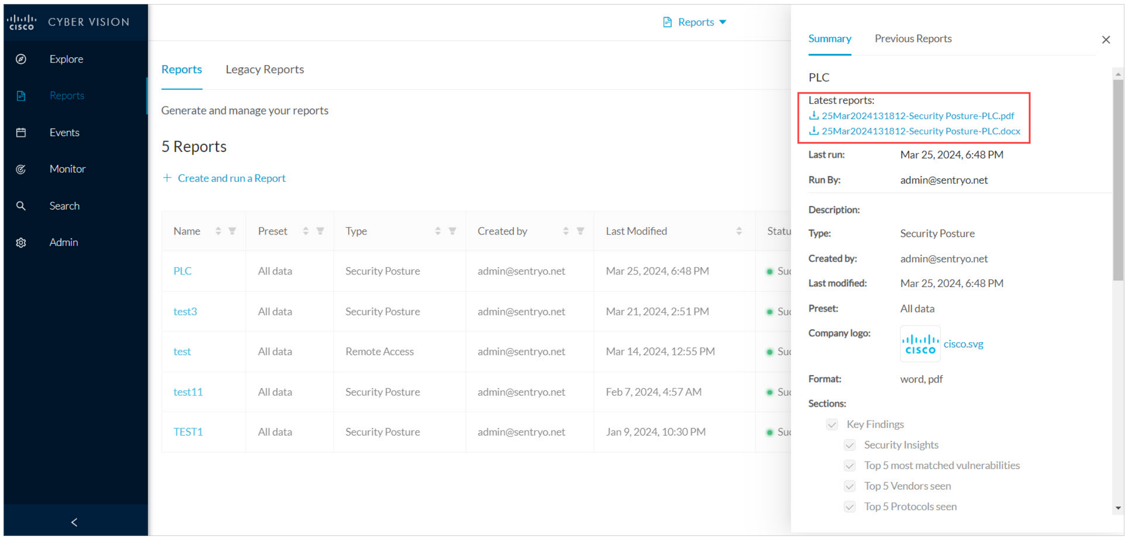
Generate and manage your reports

5 Reports

Name	Preset	Type	Created by	Last Modified	Status	Last Run	Actions
PLC	All data	Security Posture	admin@sentryo.net	Mar 25, 2024, 6:48 PM	● Success	Mar 25, 2024, 6:48 PM	···

Step 12 In the **Details** panel, click the links to download the latest reports.

The **Previous Reports** tab has older reports.



Generate and manage your reports

5 Reports

Name	Preset	Type	Created by	Last Modified	Statu
PLC	All data	Security Posture	admin@sentryo.net	Mar 25, 2024, 6:48 PM	Su
test3	All data	Security Posture	admin@sentryo.net	Mar 21, 2024, 2:51 PM	Su
test	All data	Remote Access	admin@sentryo.net	Mar 14, 2024, 12:55 PM	Su
test11	All data	Security Posture	admin@sentryo.net	Feb 7, 2024, 4:57 AM	Su
TEST1	All data	Security Posture	admin@sentryo.net	Jan 9, 2024, 10:30 PM	Su

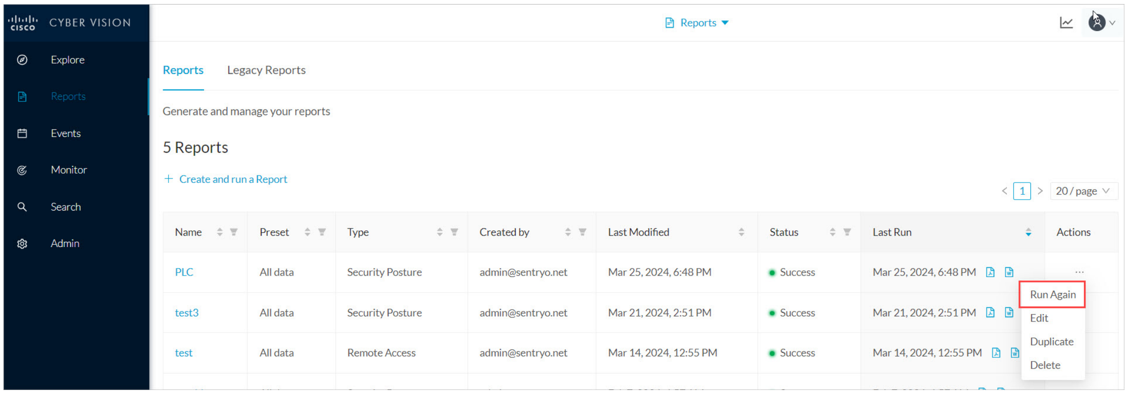
PLC

Latest reports:
25Mar2024131812-Security Posture-PLC.pdf
25Mar2024131812-Security Posture-PLC.docx

Last run: Mar 25, 2024, 6:48 PM
Run By: admin@sentryo.net

Description:
Type: Security Posture
Created by: admin@sentryo.net
Last modified: Mar 25, 2024, 6:48 PM
Preset: All data
Company logo: cisco.svg
Format: word, pdf
Sections:
- Key Findings
  - Security Insights
  - Top 5 most matched vulnerabilities
  - Top 5 Vendors seen
  - Top 5 Protocols seen

Step 13 To generate a new report, click **Run Again** under **Actions**.



Generate and manage your reports

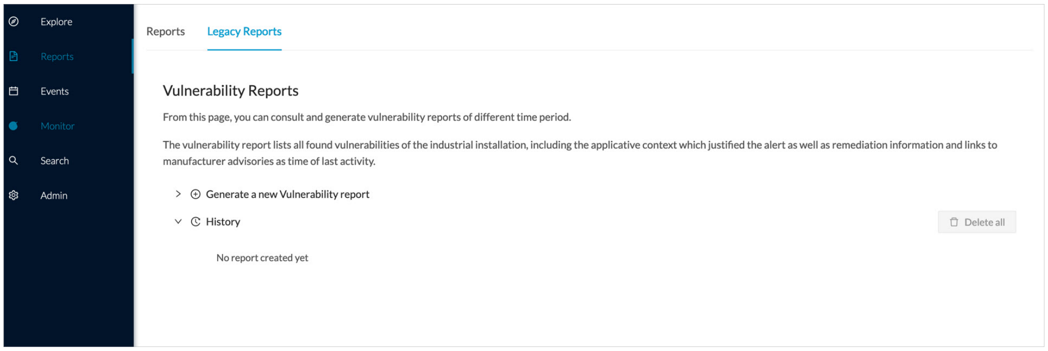
5 Reports

Name	Preset	Type	Created by	Last Modified	Status	Last Run	Actions
PLC	All data	Security Posture	admin@sentryo.net	Mar 25, 2024, 6:48 PM	Success	Mar 25, 2024, 6:48 PM	...
test3	All data	Security Posture	admin@sentryo.net	Mar 21, 2024, 2:51 PM	Success	Mar 21, 2024, 2:51 PM	
test	All data	Remote Access	admin@sentryo.net	Mar 14, 2024, 12:55 PM	Success	Mar 14, 2024, 12:55 PM	

Legacy Reports

Legacy reports are exportable files which improve your visibility of valuable information about your industrial network. Information is collected and categorized by 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).

To access **Legacy Reports**, click **Reports** from the black banner > **Legacy Reports**.



Vulnerability Reports

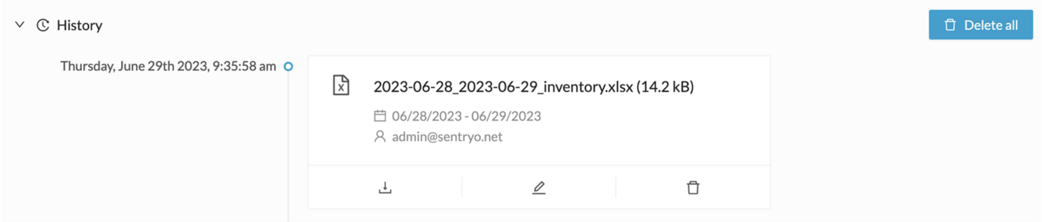
From this page, you can consult and generate vulnerability reports of different time period.

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.

No report created yet

Vulnerability report lists all components detected as vulnerable and gives further details about the vulnerabilities. Vulnerabilities are based on the Knowledge DB provided by Cisco. **Best practice:** Keep the Knowledge DB up to date, so you are 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. We strongly recommend fixing outdated states as soon as possible. Links to manufacturers' websites are provided for this purpose.

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



Thursday, June 29th 2023, 9:35:58 am

2023-06-28_2023-06-29_inventory.xlsx (14.2 kB)

06/28/2023 - 06/29/2023

admin@sentryo.net