

## VIEWING AND CREATING SUMMARY REPORTS

The Summary Reports display all report types generated for your organization.

In the MD Portal, select **Summary Reports** from the **Resources** menu to go to the **Reports** page. The **Reports** page contains created *Report Definitions* on the left side and processed *Report List* on the right side. Toggle appropriate column to order the *Report List* ascending or descending and click the **Download report** icon to download the specific report into a CSV file.

### Report Types

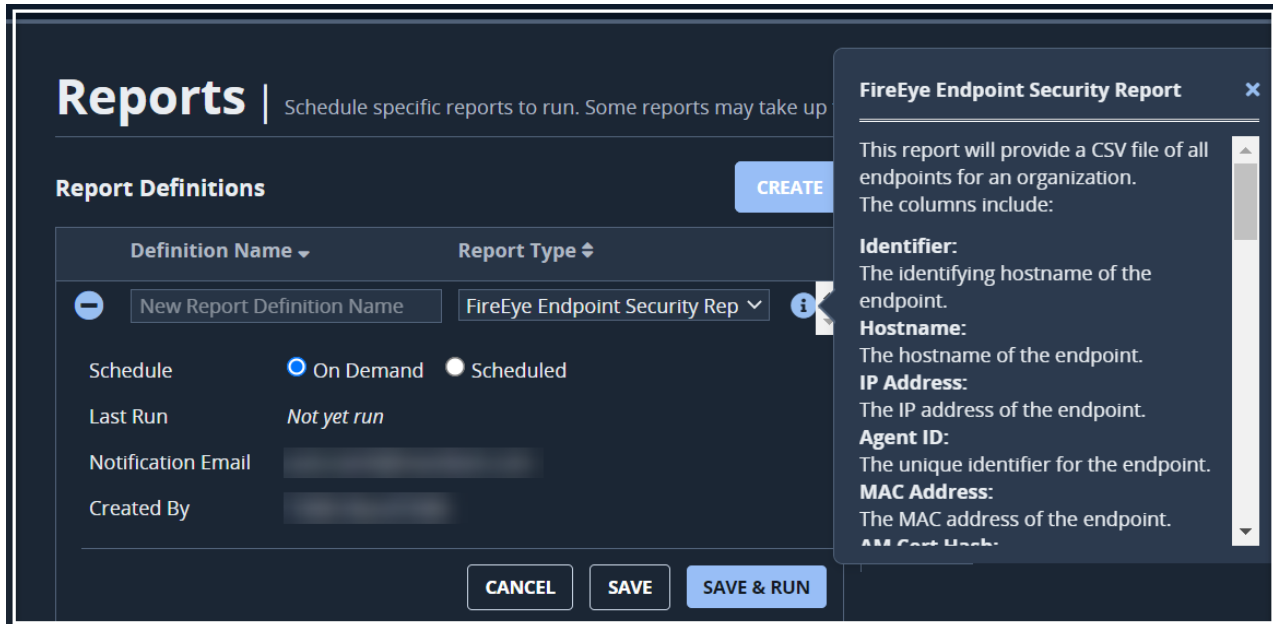
There are multiple built-in report types provided in the MD portal. Typical built-in report types include, but are not limited to, the following:

Report Type	Description
<b>Announcements</b>	This report generates a PDF that includes all the announcements published to you during the reporting period.
<b>Blogs</b>	This report generates a PDF that includes all blogs published to you during the reporting period.

Report Type	Description
<b>Trellix Endpoint Security Report</b>	<p>This report will provide a CSV file of all endpoints for an organization. The columns include:</p> <ul style="list-style-type: none"> <li>• <b>Identifier:</b> The identifying host name of the endpoint.</li> <li>• <b>Hostname:</b> The host name of the endpoint.</li> <li>• <b>IP Address:</b> The IP address of the endpoint.</li> <li>• <b>Agent ID:</b> The unique identifier for the endpoint.</li> <li>• <b>MAC Address:</b> The MAC address of the endpoint.</li> <li>• <b>Organization:</b> The client for the endpoint.</li> <li>• <b>Domain:</b> The domain of the endpoint.</li> <li>• <b>OS Patch Level:</b> The patch level of the OS running on the endpoint.</li> <li>• <b>OS Name:</b> The operating system running on the endpoint.</li> <li>• <b>Last Discovered Timestamp:</b> This is the last date and time (UTC) the endpoint checked into MD.</li> </ul> <p> <b>NOTE:</b> This value doesn't change regardless of the defined reporting period.</p> <ul style="list-style-type: none"> <li>• <b>GMT Offset:</b> This will allow you to determine the local time for the endpoint.</li> </ul> <p> <b>NOTE:</b> This value doesn't change regardless of the defined reporting period.</p> <ul style="list-style-type: none"> <li>• <b>Agent Version:</b> The version of the agent running on the endpoint.</li> <li>• <b>Containment State:</b> This flag indicates the containment state of the endpoint.</li> </ul> <p> <b>NOTE:</b> This value doesn't change regardless of the defined reporting period.</p>
<b>Investigation Monthly Metrics</b>	<p>This report generates a PDF that provides metrics around the Investigations published within the reporting period. The metrics include:</p> <ul style="list-style-type: none"> <li>• Number of Investigations by severity</li> <li>• Number of Investigations by status (open / closed)</li> <li>• Number of Investigations by source (network / endpoint / other)</li> <li>• Average time to assignment</li> <li>• Average time to resolution</li> </ul>
<b>Dashboard</b>	<p>This report generates a PDF of the information shown on the dashboard.</p> <p> <b>NOTE:</b> This report will show the information over the last 30 days regardless of the reporting period selected.</p>

Click the **i** (information) button during report creation for any Report Type selected from the drop down list to view the

detailed description of the selected report type along with its fields and associated notes.



The screenshot displays the 'Reports' section of the Mandiant interface. The main area is titled 'Report Definitions' and contains a table with columns for 'Definition Name' and 'Report Type'. A 'CREATE' button is visible in the top right of this section. Below the table, there are fields for 'Schedule' (with radio buttons for 'On Demand' and 'Scheduled'), 'Last Run' (showing 'Not yet run'), 'Notification Email', and 'Created By'. At the bottom of the main area are 'CANCEL', 'SAVE', and 'SAVE & RUN' buttons.

A modal window titled 'FireEye Endpoint Security Report' is open on the right side. It contains the following text:

**FireEye Endpoint Security Report** ✕

This report will provide a CSV file of all endpoints for an organization. The columns include:

- Identifier:** The identifying hostname of the endpoint.
- Hostname:** The hostname of the endpoint.
- IP Address:** The IP address of the endpoint.
- Agent ID:** The unique identifier for the endpoint.
- MAC Address:** The MAC address of the endpoint.
- Alert Hash:**

### Creating Reports

You can create any report type by using the Create Report feature in the **Reports** page.

**MANDIANT ADVANTAGE** | **MANAGED DEFENSE**

# Reports

 | Schedule specific reports to run. Some reports may take up to 2 hours to complete.

## Report Definitions

CREATE

Definition Name  Report Type

Data Date Range

Appendix

Schedule  On Demand  Scheduled

Start / End Date:

Frequency

Daily

Weekly

Monthly

Interval

Every  day(s).

Last Run *Not yet run*

Notification Email

Created By

CANCEL SAVE SAVE & RUN

**TO CREATE A SUMMARY REPORT:**

1. In the MD Portal, select **Summary Reports** from the **Resources** menu.
2. Click **CREATE**.
3. Type the Definition Name.
4. Select the Report Type.
5. Select On Demand or Scheduled.

- a. If you select scheduled, select your report Start / End Date.
- b. Select a date range between 0 to 30 days.



**NOTE:** Reports that extend longer than 30 days may time out.

- c. Select the Frequency and the Interval.

6. Click **SAVE** or **SAVE & RUN**.



**NOTE:** Some reports may take up to 2 hours to generate depending on your parameters.