

This feature is only available for our [commercial versions](#).

- [Intro](#)
- [Requirements](#)
- [Managing Executive Reports](#)
- [Making a Report](#)
- [Eliminating a Report](#)
- [Templates](#)

Intro

No more 3AM reporting!

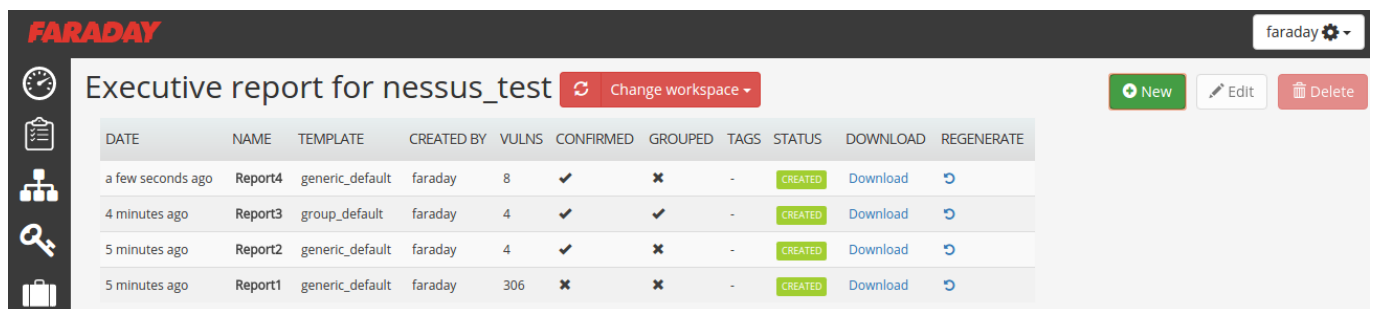
The Executive Reports feature lets you create (as the name implies) reports using the results obtained in each workspace. When an Executive Report is created, all the data from the Status Report is automatically processed and placed in a Word compatible document that can then be downloaded.

Requirements

To utilize this feature follow the necessary steps on our [start up configuration](#).

Managing Executive Reports

To manage your reports you need to access Faraday's Web Interface and click on **Executive Report** icon (the one that looks like a suitcase).

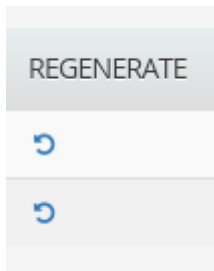


DATE	NAME	TEMPLATE	CREATED BY	VULNS	CONFIRMED	GROUPED	TAGS	STATUS	DOWNLOAD	REGENERATE
a few seconds ago	Report4	generic_default	faraday	8	✓	✗	-	CREATED	Download	↻
4 minutes ago	Report3	group_default	faraday	4	✓	✓	-	CREATED	Download	↻
5 minutes ago	Report2	generic_default	faraday	4	✓	✗	-	CREATED	Download	↻
5 minutes ago	Report1	generic_default	faraday	306	✗	✗	-	CREATED	Download	↻

All the reports will be listed, including their info, status and link to download.

To edit a report, select it and click on the **Edit** button. A modal will appear allowing you to modify all the report fields. Save it and a brand new report will be generated, keeping the original version intact.

If, instead, you want a new report that is exactly like an existing one but with the current data of your workspace, you can click on the **Regenerate** button in the reports list.



Reports can only be regenerated one at a time, so the regeneration buttons are disabled while this action is being performed.

Making a report

To create a new report, navigate to the Executive Report component and click on **New**. A form will open asking for the following fields:

- **Report name** - this will be used to name the report file.
- **Use only confirmed vulns for this report** - if this checkbox is *selected*, no false positives will be present in the final report.
- **Tags** - when selected, vulnerabilities will be filtered by the selected tag. If more than one tag is selected, all vulns containing one of those will be present in the final report.
- **Template** - select the template to use as a base for your report. Depending on the selected dataset the options will change
- **Grouped report** - select this option to generate a report using a grouped dataset.
- **Title** - this is the name that will be used to create the cover of the report.

The following are a sort of placeholder fields for information that's commonly added to most reports. They are text fields and can be used for any relevant information, not just for what they're named after: * **Scope** * **Objectives** * **Summary** * **Conclusions** * **Recommendations**

Executive report for ws1

CancelOK

report4

☐ Use only confirmed vulnerabilities for this report

Tags

If one or more tags are selected the report will be generated using vulnerabilities that includes them.

caseyfrankierorysam

Template

☐ Grouped report

generic brief.docx

Summary

The following report includes **37** vulnerabilities , **1** is critical , **15** are high , **1** is medium , **6** are low , **14** are info

Title. e.g.: 'Network XYZ'

Client Name. e.g. 'ACME INC'

Scope

Objectives

Faraday processes all the information and spits out a shiny new report that is automatically available for download.

Dolor sit amet

Lorem Ipsum

February 2017

Document Confidentiality: All information contained in the present report will remain strictly confidential. It is prohibited to copy and reproduce this document or a part of it without the expressed consent of Infobyte Security Research, even after the expiration and termination of the use of the present proposal.

Filtering

There are two main ways to manage the data that goes into the final report - *confirming vulns* and **tagging them**.

By default all of the vulnerabilities added manually are set as *confirmed* and all of those added by a Plugin are set as *false positives*. If the checkbox "use only confirmed vulns" is selected, the report will only contain confirmed findings.

If you need a custom report that includes only some of the findings in the workspace, you can also

tag the desired vulnerabilities and then create a report only with that tag.

At least one vulnerability must be tagged in order to have the option to generate a tag-filtered report. When the form opens an option to select tags will appear. Keep in mind that one or more tags can be selected.

These two parameters (confirmed and tags) can be mixed to create different outcomes.

Executive report for test1

report2

☐ Use only confirmed vulnerabilities for this report

Tags

If one or more tags are selected the report will be generated using vulnerabilities that includes them.

dbowman jbauer

Template

☐ Grouped report

generic default.docx

Summary

The following report includes 39 vulnerabilities , 1 is critical , 5 are medium , 3 are low , 30 are info

Title. e.g.: 'Network XYZ'

Eliminating a report

From the Executive Report window, select the document and click on **Delete**

Delete

Templates

All report templates are located in `reports/executive/templates` in your Faraday installation directory. The default one is `generic_default.docx`, you can modify it to get customized reports.

You can download an example report [here](#) and its corresponding template [here](#).

The template uses Jinja2 syntax so we strongly recommend reading the [official documentation](#) before modifying the document. The library used to create the report is **python-docx-template** available via [Github](#). All Jinja2 tags are available, although there are some [restrictions](#).

An example of how the template cover looks like

{{enterprise}}

{{ title|e }}

{{ date|datetimeformat('%B %Y') }}

Document Confidentiality: All information contained in the present report will remain strictly confidential. It is prohibited to copy and reproduce this document or a part of it without the expressed consent of InfoByte Security Research, even after the expiration and termination of the use of the present proposal.

Datasets

Faraday provides two different datasets to create Executive Reports - **generic** and **grouped**.

The *generic dataset* provides one entry for each individual vulnerability with all of its fields readily available as a dictionary. The field **parent** contains an ID corresponding to the vulnerability's parent (either a Host or a Service).

The *grouped dataset* groups vulnerabilities by **name** and **description**. If two or more vulnerabilities share the same name and description, they will be presented as one. The field **parent** contains a Python Dictionary-style object with the parent IDs as keys and a Python Dictionary-style object containing **evidence_subdoc**, **data** and **target** as values. **Tags** and **references** will be merged for vulnerabilities that are grouped and not separated by parent.

By default all of the reports are created using the *generic dataset*. To create a report using the *grouped dataset*, select the checkbox "grouped report" when creating it, as shown below.

Template

☒ Grouped report

group default.docx ▼

Keep in mind that each template should be designed for a specific dataset and that these are not interchangeable.

Naming

If you want to add a new template make sure to follow the naming guidelines as follows.

- **generic_{customName}.docx** for generic reports - all the vulnerabilities will be listed as individual items in these reports
- **group_{customName}.docx** for grouped reports - vulnerabilities will be grouped by name and description

Data

The data available to the Report template is:

- **conclusions** - contains the text loaded when creating the report
- **counter_severity** - a dictionary with all the severities and the amount of vulns for each one
- **date** - the date when the Report was created, as the name of the month and four digits for the year
- **enterprise** - contains the text loaded when creating the report
- **hosts** - a dictionary with all the hosts in the Workspace
- **hosts_amount** - an int containing the amount of hosts in the Workspace
- **objectives** - contains the text loaded when creating the report
- **overview_images** - a sub-document containing vulnerability piecharts
- **recommendations** - contains the text loaded when creating the report
- **scope** - contains the text loaded when creating the report
- **services** - a dictionary with all the services in the Workspace
- **services_amount** - an int containing the amount of services in the Workspace
- **summary** - contains the text loaded when creating the report
- **title** - contains the text loaded when creating the report
- **vulns** - a dictionary with all the vulnerabilities in the Workspace except for vulns with severity *unclassified*, which are not included
- **vulns_amount** - an int containing the amount of vulnerabilities in the Workspace except for vulns with severity *unclassified*, which are not included

Grouped reports will have an additional field:

- **vulns_grouped_amount** - an int containing the total amount of vulnerabilities after grouping