BigFix Reports

User’s guide v1.0.2

This guide is intended to help you understand how to interact with BigFix Reports interface and the features released.

INTRODUCTION

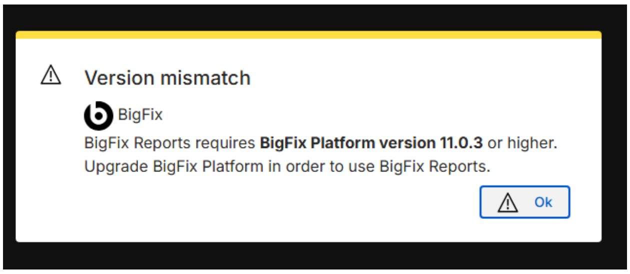
BigFix Reports is a new modern interface to create reports out of data that can originate from multiple data sources. Like Web Reports, it can be used by all BigFix users (personas) and data visibility is assessed accordingly.

This guide focuses on the content of the first generally available version.

The way to navigate the interface is through the left-hand menu which can be collapsed to save space, as well as the global navigation on top of the page.

PREREQUISITES

To run BigFix Reports v1.0, you need to have BigFix Platform v11.0.3 or higher. If this prerequisite is not met, and you had previously enabled the BigFix Report Preview, the user will be presented with a modal explaining the requirement and will not be able to use the application if platform is not upgraded.



⚠ Version mismatch

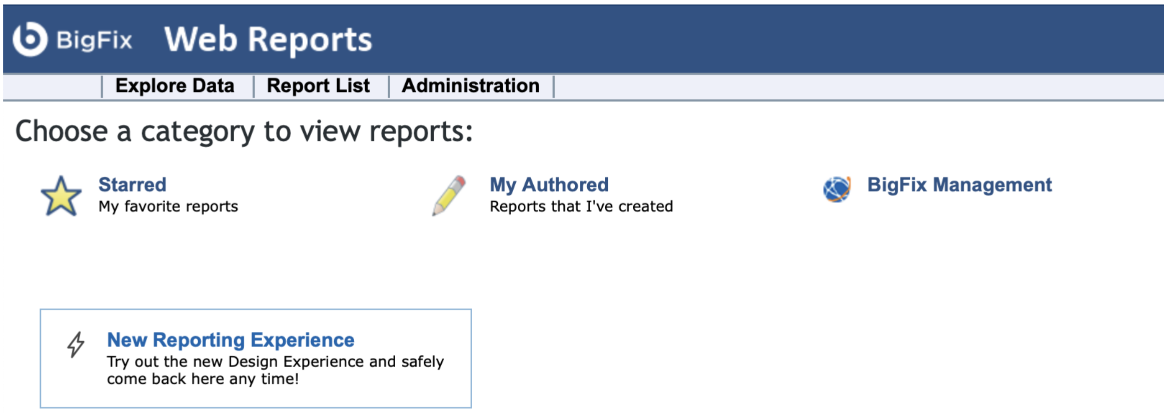
BigFix

BigFix Reports requires **BigFix Platform version 11.0.3** or higher.
Upgrade BigFix Platform in order to use BigFix Reports.

INSTALLATION / LICENSING

BigFix Reports site is part of all our basic offers. You need to accept the license of an available product in your License Dashboard, and then Enable the BigFix Reports site.

To navigate to the new BigFix Reports web interface, simply launch the Web Reports application, and from there you should be able to view a new panel in the homepage: just follow up the instructions and you will be redirected to the new UI.



BigFix Web Reports

Explore Data | Report List | Administration

Choose a category to view reports:

Starred
My favorite reports

My Authored
Reports that I've created

BigFix Management

New Reporting Experience
Try out the new Design Experience and safely come back here any time!

USERS

For this first release, Web Reports users can access the BigFix Reports application, and they will inherit authorization and visibility of BigFix data they are assigned in BigFix. In the future releases, user management will be independent.

COMPATIBILITY BETWEEN WEB REPORTS AND BIGFIX REPORTING

BigFix reporting is enhancing the concept of report and is changing a few capabilities to allow exploitation by multiple applications in the future and flexible enough to accommodate the new concept of playlist. Over time the structure of the report will evolve, hence will not be compatible any longer with the existing Web Reports structure, keeping the value for the users that current reports provide but possibly make it more flexible.

We guarantee that existing reports are visible in the new application but the user should avoid making changes to the same report from multiple interfaces

Example: I am in the new interface, and I pick up a report I created in Web Reports and start changing it

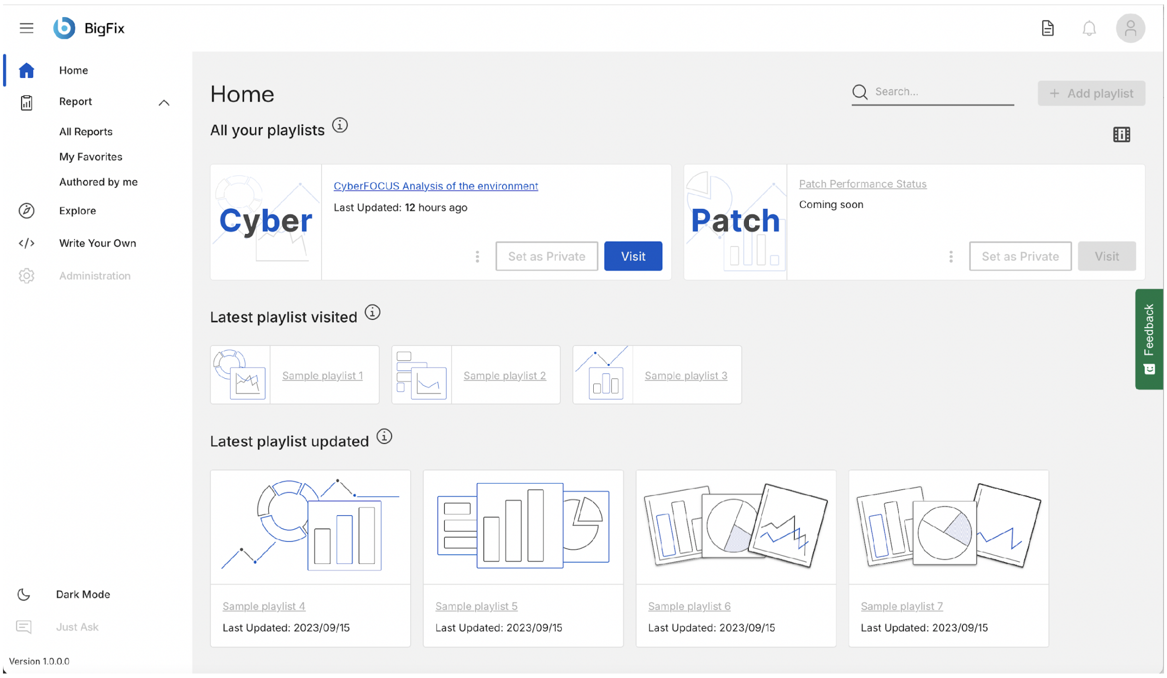
- For Computer and Custom reports, changes are visible in both interfaces
- For Content, Actions and Operators:
    - Changes in the data grid will NOT be reflected in Web Reports
    - Changes to charts will NOT be reflected in Web Reports
    - Changes to filters are reflected in Web Reports

SCENARIOS

Let’s see how to use BigFix Reports, by scenarios. Please note that each main page has a link to a short video to explain its features. The icon is 🎞 and by clicking it you will be redirected to an external video streaming site. Therefore, if your computer browser does not have internet connection the video cannot be viewed.

(A) The user lands on the home page - explore the playlists

The home page of BigFix Reports gives you an overview of the playlists available. Imagine you are reading your favorite newspaper with headlines on the news of the day



The concept of **playlist** has been introduced to indicate a new object like a collection view of reports widgets that might harvest from all the different family areas.

The objective is to create a holistic view tailored to specific stakeholders for whom you might need to convey key messages about the security posture, or device landscape.

It represents an abstraction layer on top of reports, to facilitate sharing of the information BigFix is capable to provide. It makes BigFix visibility tangible.

Having the possibility of creating playlists, along with a continuous stream of playlists that will be produced over time and gathered with the BigFix Reports site, reduces the need for learning how to create custom reports as well.

Moreover, the concept of playlist is inherited by the usual streaming media usage and as such it should convey the message of customizability and flexibility.

The home page is divided into three main parts.

On top, you find the two playlists that by default BigFix Reports provides. Over time we will make this section customizable with the playlist chosen by you. The playlists are then listed by last access time and by the last update. New playlists added by BigFix in the updates will be highlighted as new.

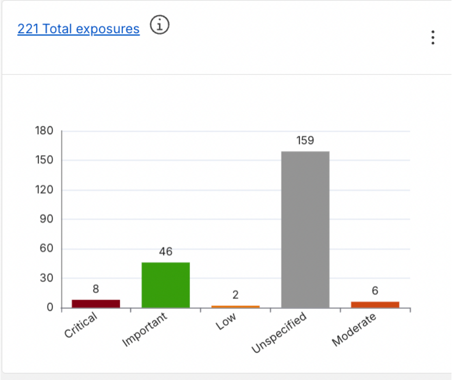
Playlists can be browsed. In the first release of BigFix Reports, only CyberFocus and PatchFOCUS are available. Over time more playlists will be provided as content.

CyberFOCUS Playlist

Represents a collection of metrics and KPIs related to cybersecurity. It bridges the gap between IT and security with focus on vulnerabilities (CVEs) and suggests how BigFix can help mitigate these vulnerabilities.

Note: to have access to this report, the user must be subscribed to CyberFOCUS site. Additionally, if the user is entitled to the CISA Known Exploited Vulnerabilities content pack, additional playlist tiles will be visible.
Documentation available in the official BigFix documentation site at this link.
This playlist gives security insights retrieved by BigFix patch related content.
Let’s see in detail what the various widgets represent.

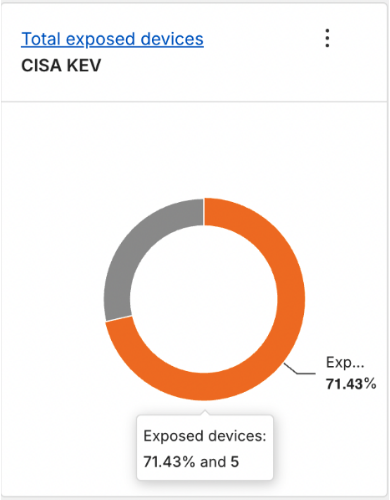
Total exposures: distribution of exposures by severity.This chart takes into consideration all patches of all subscribed sites and represents the aggregate amount of exposures across all devices in the environment. An exposure is considered a single instance of a missing patch per machine. For example: if one device is missing three patches, this would equate to 3 exposures. If three devices were to be missing 3 patches each, this would equate to nine exposures. The graph provided will look as follows



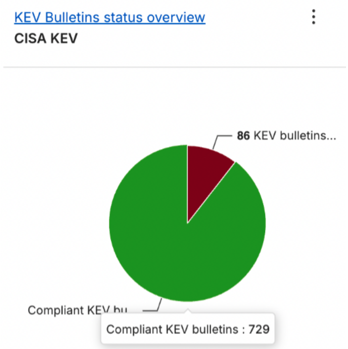
The next two charts in the screen below are visible only if the user is subscribed to the CISA KEV (Known Exploited Vulnerability) site. In this case BigFix Reports can get more information about vulnerabilities in context to the CISA KEV specification. This site is an add-on content pack. More information is in the documentation page. The KEV dimension helps with prioritization by listing CVEs known to have been actively exploited.

Total exposed devices: This chart shows the number of devices exposed to at least one CVE from the CISA KEV List. It also indicates the number of devices that are fully compliant with the KEV content site, meaning they are subscribed to the KEV content pack but are not applicable to any content associated with it.

This graph includes all KEV content, both open and past due, and does not filter by KEV bulletin suspense date.



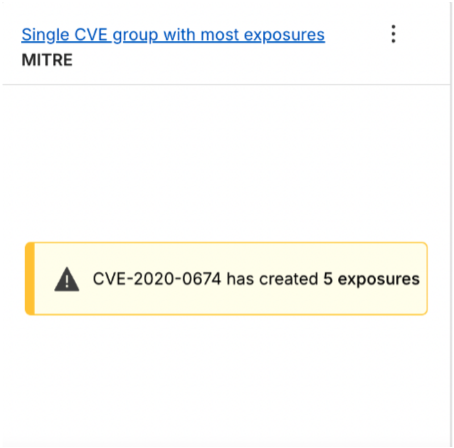
KEV Bulletins status overview: This graph displays the compliance status of KEV bulletins that have passed their suspense dates. CISA assigns a suspense date to each KEV vulnerability, which is the deadline for complete remediation to ensure compliance. This chart shows the system’s compliance for all bulletins that have exceeded their suspense dates.



KEV Bulletins status overview

CISA KEV

Single CVE group with most exposures: This chart shows the CVE with the most exposures that has been associated with a MITRE APT Group.

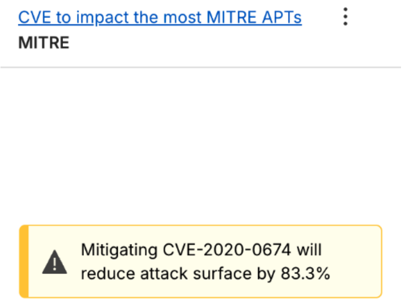


Single CVE group with most exposures

MITRE

CVE-2020-0674 has created 5 exposures

CVE to impact the most MITRE APTs: This chart identifies the CVE with the highest accumulated weight, based on its exposures and associations with MITRE APT groups. The accumulated weight is calculated by multiplying the number of exposures by the number of associated groups. For example, a CVE associated with 5 MITRE APT groups and having 5 exposures will have an accumulated weight of 25. Conversely, a CVE associated with 1 MITRE APT group and having 5 exposures will have an accumulated weight of 5. This chart highlights the CVE with the highest accumulated weight. The provided percentage represents the potential reduction in total applied weight that can be achieved by mitigating this one CVE.

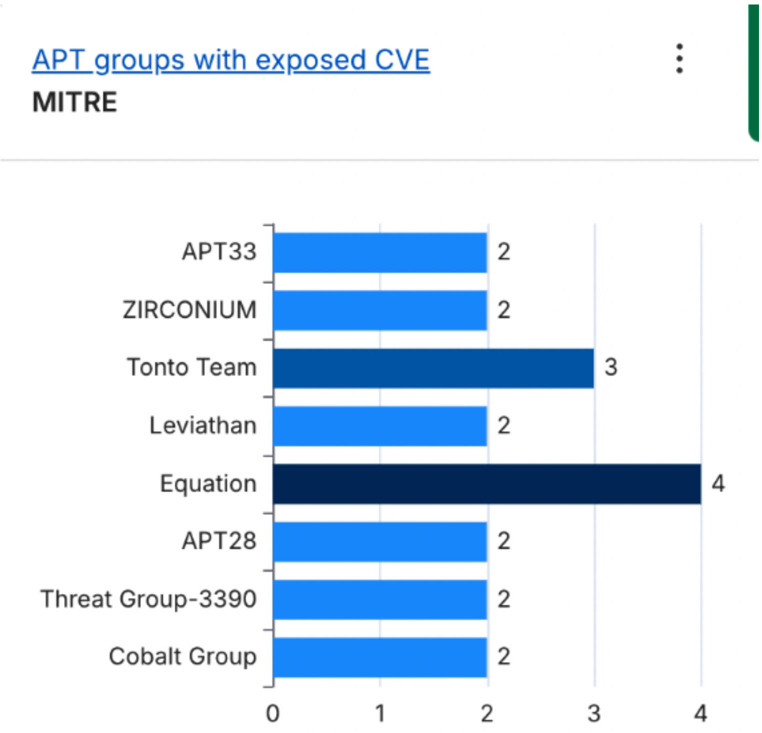


CVE to impact the most MITRE APTs

MITRE

Mitigating CVE-2020-0674 will reduce attack surface by 83.3%

APT groups with exposed CVE: This chart displays the total number of exposures associated with CVEs linked to specific MITRE APT groups. MITRE analysis indicates that APT groups often target a specific set of vulnerabilities (CVEs). A single APT group can be associated with multiple CVEs. Each CVE can be linked to one or more fixlets, and each fixlet can be relevant to one or more machines. An exposure is defined as a single instance of a machine being applicable to a given fixlet. This chart shows the aggregate number of exposures by APT group.



APT groups with exposed CVE

MITRE

Patch Performance Playlist

Represents a collection of metrics and KPIs related to the patching process performance.

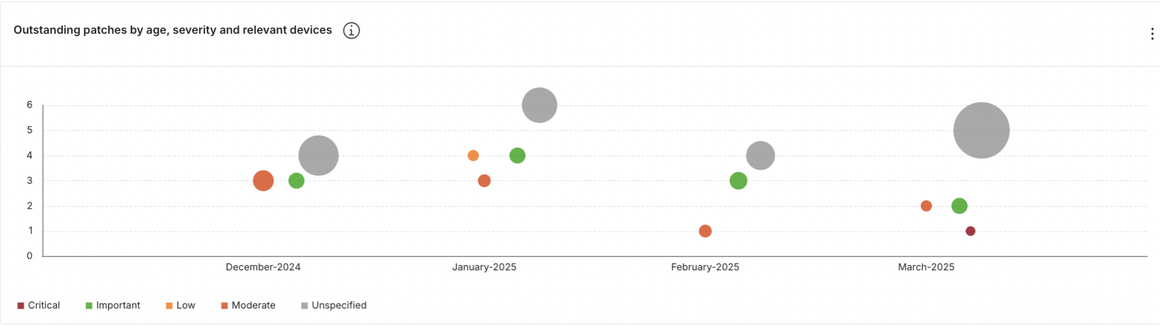
Note: to have access to this report, the user must be subscribed to at least one patch site and at least one device must be subscribed to that site. In addition, you must be subscribed to CyberFOCUS site.

Let’s see in detail what the various widgets represent. Please not that in this version the view is related to all computers: in the future, filtering by computer groups will be possible.

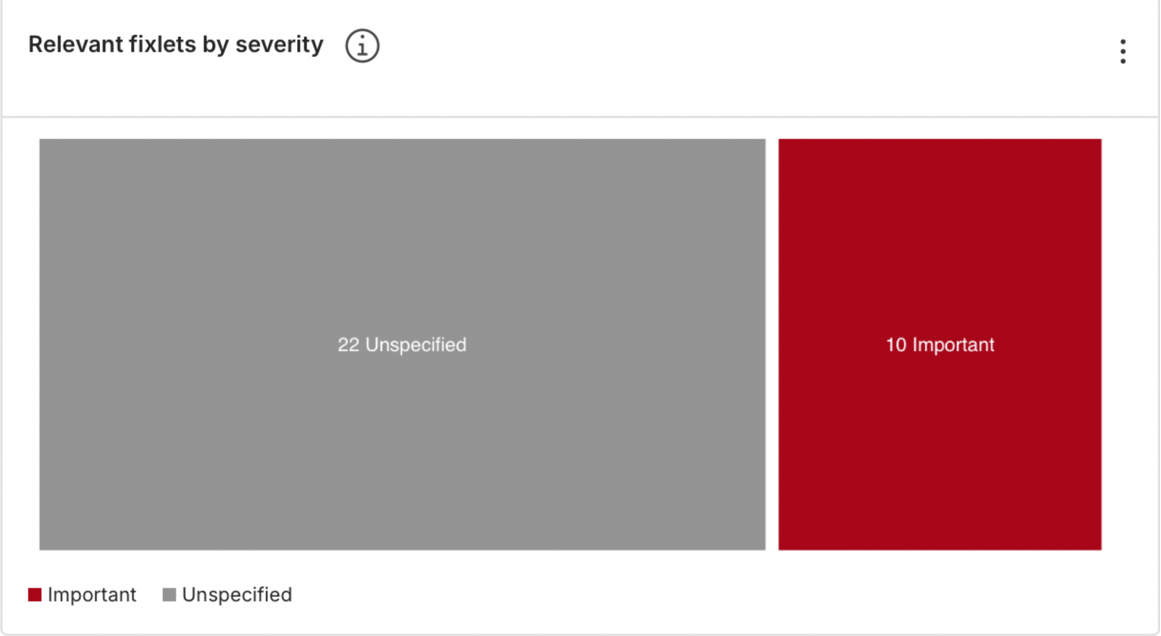
Charts are divided in three groups; the first three charts are a view by content. There is a filter on severity by which the user can customize the content to be shown in the charts. The second is about devices, the third is by site.

View by content

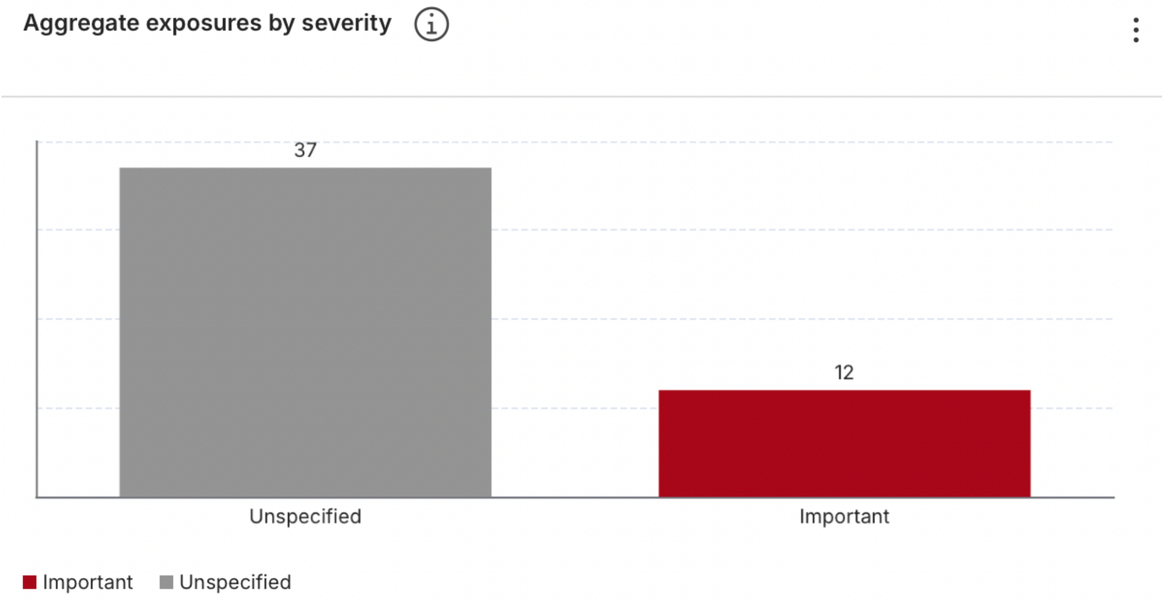
Outstanding patches by age, severity and relevant devices: This chart gives a view of patches that became first relevant in the past 4 months and are still relevant. The radius of the bubble represents the number of fixlet, the color indicates the severity as per the legenda, and the position on the Y axis represents the number of relevant devices.



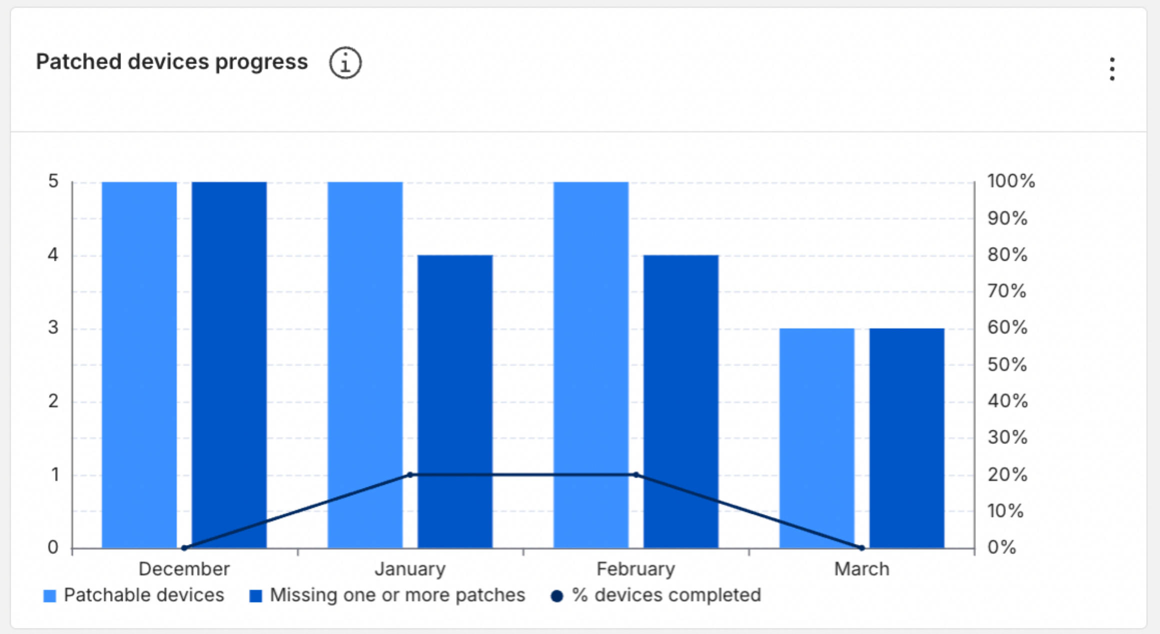
Relevant fixlet by severity: This chart gives a view of all by severity at the present time, regardless when they first became relevant



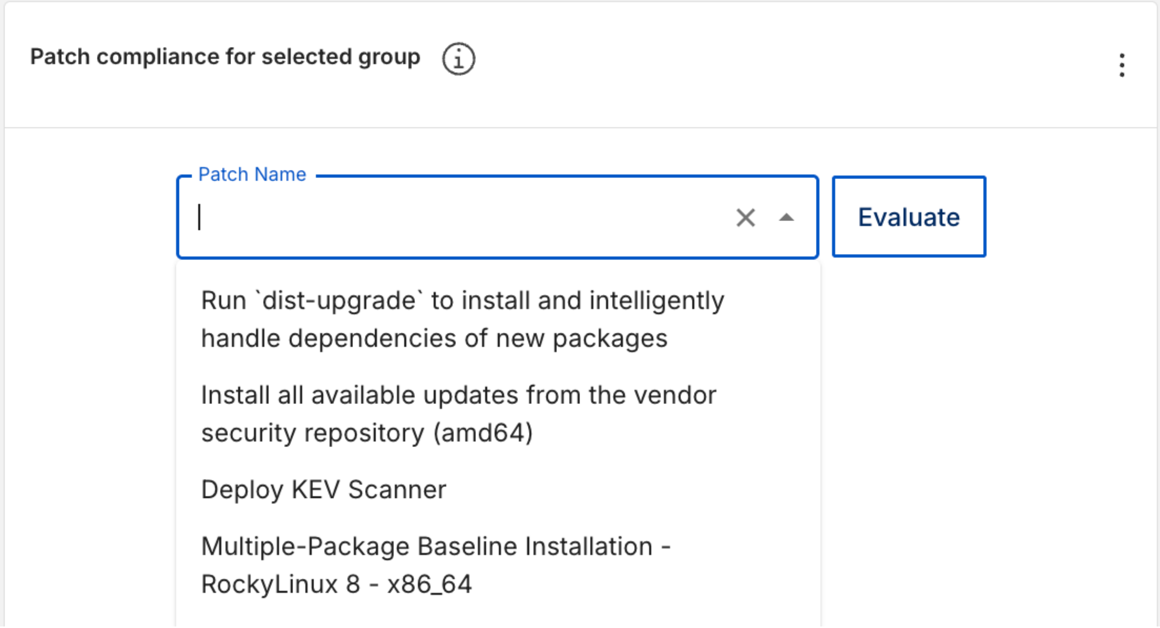
Aggregated exposures by severity: This chart gives a view of the number of exposures by severity, meaning the number of times a patch of a certain severity is relevant



Patched devices progress: This chart gives a view of the overall progress in terms of number of patched devices in the last 4 months.



Patch compliance for selected group: A simple interface to query for a specific patch to identify relevant devices. The number of devices is a link to the device view filtered by this criteria (relevance to the requested patch)



Run `dist-upgrade` to install and intelligently handle dependencies of new packages

Install all available updates from the vendor security repository (amd64)

Deploy KEV Scanner

Multiple-Package Baseline Installation - RockyLinux 8 - x86_64

Patch performance by site: This view is by site, hence is a view by platform. The concept the score has been introduced, to help the user prioritize the activities according to criteria.

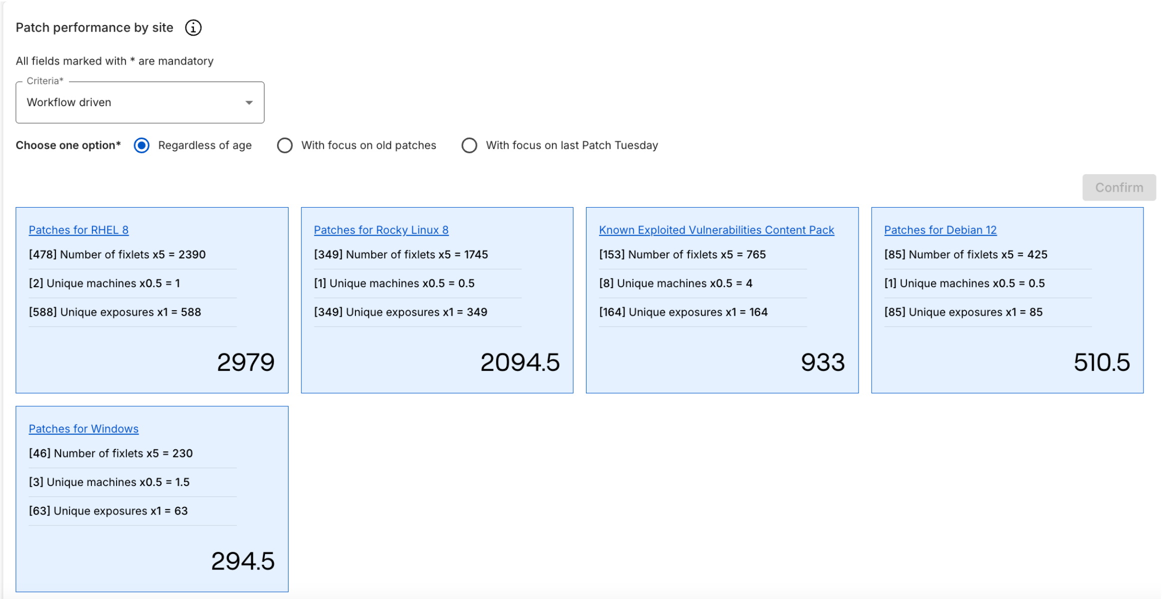
Calculate a score by patch site to highlight areas of attention, divided by platform. Depending on your priorities you can choose to give more importance to the amount of work to be done to be in compliance, translated in how many fixlets are yet to be deployed, or if you prefer to have a risk based view.Each choice brings weights to the KPI that most contribute to that score. Details on how the score is calculated are reported into every tile. If you choose "Workflow driven" criteria you can further decide if you want to calculate it by :

- regardless of age (default)
- with focus on old patches (patches publish date older than 90 days)
- with focus on last patch Tuesday (if you have Windows, patches included in last patch Tuesday yet to be installed)

If you choose "Risk driven" criteria you can further decide if you want to calculate it by:

- relevant patches belonging to a KEV or MITRE list
- patch surface
- patch vectors

Tiles are ordered in descending values of score. If you want to redo the calculation based on a different criteria, after your choice yu need to press “Confirm”.



Patch performance by site

All fields marked with * are mandatory

Criteria*: Workflow driven

Choose one option*: ● Regardless of age ○ With focus on old patches ○ With focus on last Patch Tuesday

Patches for RHEL 8
[478] Number of fixlets x5 = 2390
[2] Unique machines x0.5 = 1
[588] Unique exposures x1 = 588
2979

Patches for Rocky Linux 8
[349] Number of fixlets x5 = 1745
[1] Unique machines x0.5 = 0.5
[349] Unique exposures x1 = 349
2094.5

Known Exploited Vulnerabilities Content Pack
[153] Number of fixlets x5 = 765
[8] Unique machines x0.5 = 4
[164] Unique exposures x1 = 164
933

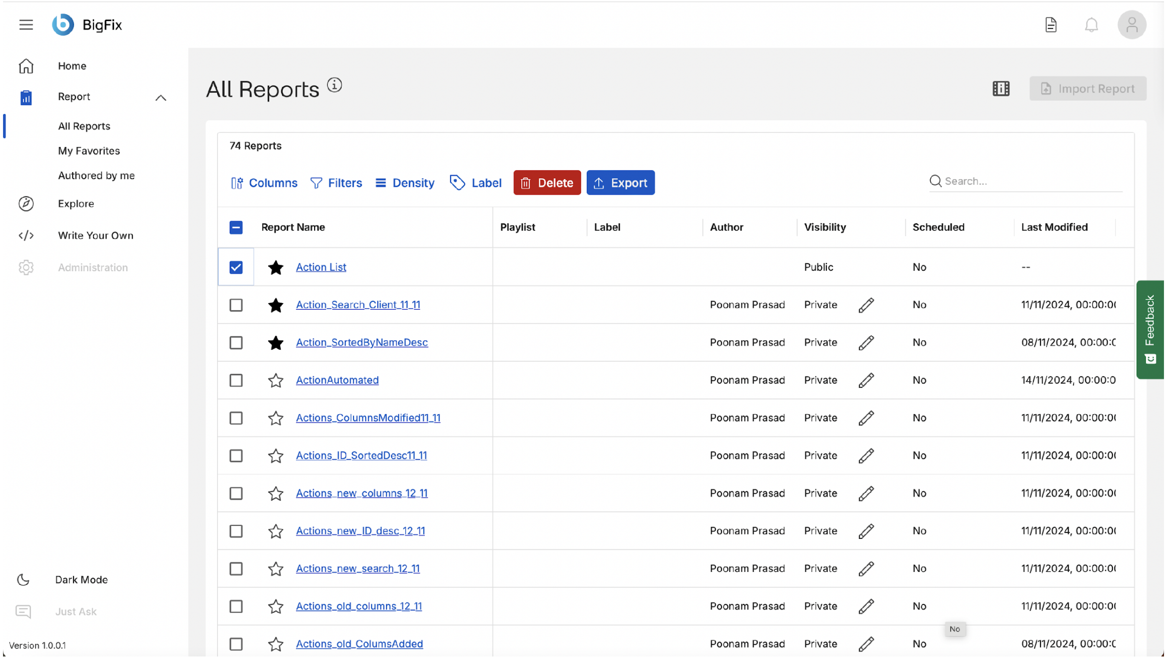
Patches for Debian 12
[85] Number of fixlets x5 = 425
[1] Unique machines x0.5 = 0.5
[85] Unique exposures x1 = 85
510.5

Patches for Windows
[46] Number of fixlets x5 = 230
[3] Unique machines x0.5 = 1.5
[63] Unique exposures x1 = 63
294.5

Note that tiles in this section provide insight for the sites Patches for, Updates for, and Known Exploited Vulnerabilities Content Pack.
The number of fixlets shown in the tiles refers to a subset of the fixlets available in the corresponding site. Fixlets must be relevant, not superseded or maintenance, and their category must belong to Update, Security, Upgrade, Fix, Advisory, and Enhancement. Moreover, the score is normalised by the number of subscribed devices to that specific site.

(B) I want to see the reports currently available, search, mark as favorite, change visibility, delete and label them

On the left-hand navigation bar, go to Reports -> All Reports



All Reports

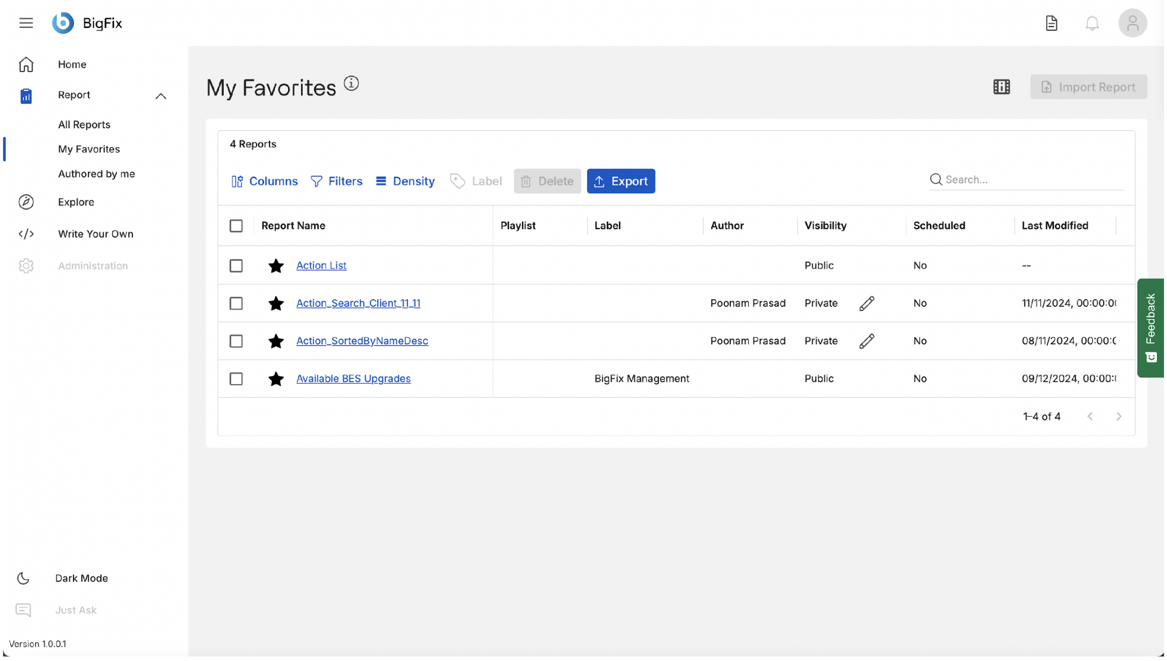
74 Reports

▬		Report Name	Playlist	Label	Author	Visibility		Scheduled	Last Modified
☑	★	Action List				Public		No	--
☐	★	Action_Search_Client_11_11			Poonam Prasad	Private	✎	No	11/11/2024, 00:00:0
☐	★	Action_SortedByNameDesc			Poonam Prasad	Private	✎	No	08/11/2024, 00:00:
☐	☆	ActionAutomated			Poonam Prasad	Private	✎	No	14/11/2024, 00:00:0
☐	☆	Actions_ColumnsModified11_11			Poonam Prasad	Private	✎	No	11/11/2024, 00:00:0
☐	☆	Actions_ID_SortedDesc11_11			Poonam Prasad	Private	✎	No	11/11/2024, 00:00:0
☐	☆	Actions_new_columns_12_11			Poonam Prasad	Private	✎	No	11/11/2024, 00:00:0
☐	☆	Actions_new_ID_desc_12_11			Poonam Prasad	Private	✎	No	11/11/2024, 00:00:0
☐	☆	Actions_new_search_12_11			Poonam Prasad	Private	✎	No	11/11/2024, 00:00:0
☐	☆	Actions_old_columns_12_11			Poonam Prasad	Private	✎	No	11/11/2024, 00:00:0
☐	☆	Actions_old_ColumsAdded			Poonam Prasad	Private	✎	No	08/11/2024, 00:00:

The list is displayed in a data grid, you can get familiar with the customization of the data table, sorting of columns content, personalization in terms of columns, reordering of columns through drag and drop. Or you can search a string using the Search field to identify reports with matching name or any other property. The table can be exported in CSV format at your convenience.

Note: for this release, personalization to the view is not persistent per user. It will once user management is added.

When creating a report, by default it is set as Private but you can edit the Visibility value to change it to Public. If you are the owner you can revert back a Public report to be Private. Users with Administrator permission have full control over the reports.



☐	Report Name	Playlist	Label	Author	Visibility	Scheduled	Last Modified
☐	★ Action List				Public	No	--
☐	★ Action_Search_Client_11_11			Poonam Prasad	Private	No	11/11/2024, 00:00:0
☐	★ Action_SortedByNameDesc			Poonam Prasad	Private	No	08/11/2024, 00:00:
☐	★ Available BES Upgrades		BigFix Management		Public	No	09/12/2024, 00:00:

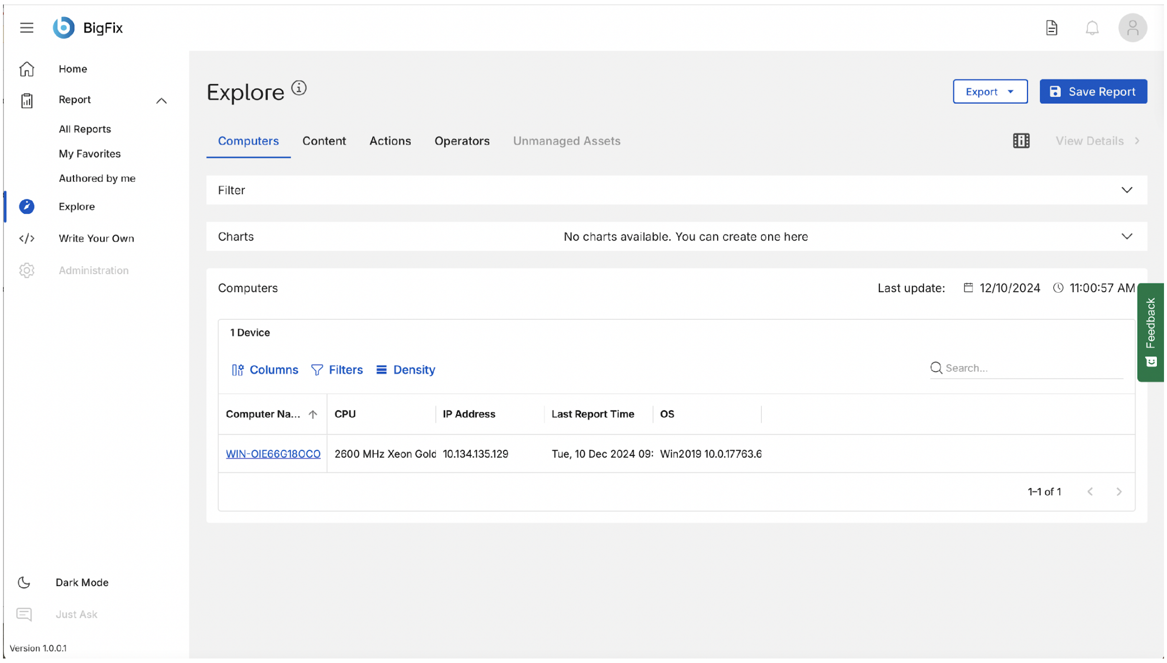
By clicking the star icon, you can set a report as favorite, and you can access all the favorite reports with the quick link on the left menu “My Favorite”.
An additional quick link is “Authored by me” to have access to the list of reports you created.

Selecting one or more reports the button “Label” will activate and by pressing it you can manage the labels associated with that report by adding and removing. Users can only delete labels they have created but can use labels set by any other user. Only if administrator role is assigned, the user can manage all of them.

Selecting one or more reports enables the Delete button. Upon confirmation you can proceed to delete the reports if you have authority, i.e. you are the owner of the report.

(C) I want to create a new report on computers / content / actions / operators, export it and save it

On the left-hand navigation bar, go to Explore. A page with multiple tabs will help you creating a report out of a determined data type. You can create reports for Computers, Content, Actions, Operators.



No charts available. You can create one here

Computers Last update: 12/10/2024 11:00:57 AM

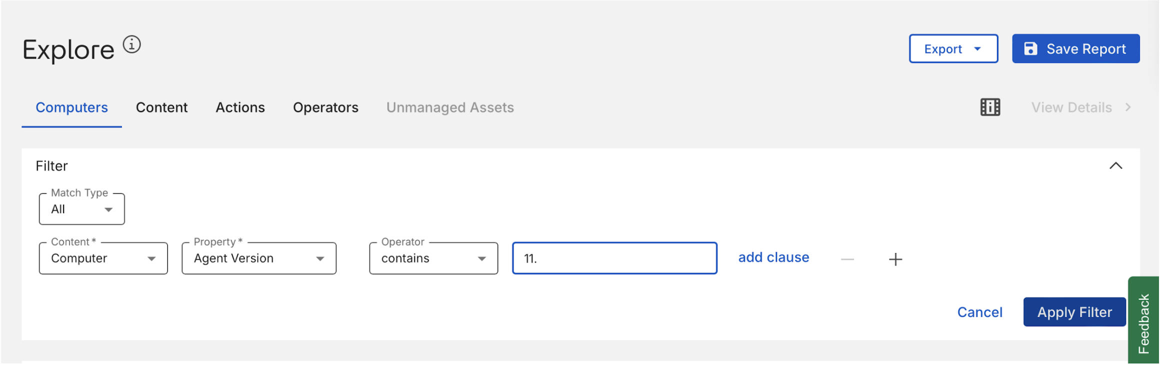
1 Device

Computer Na...	CPU	IP Address	Last Report Time	OS
WIN-OIE66G18OCO	2600 MHz Xeon Gold	10.134.135.129	Tue, 10 Dec 2024 09:	Win2019 10.0.17763.6

1–1 of 1

You should now be familiar with the data table capabilities, like filtering data or sorting, adjusting table content in terms of columns and such.

A filter section is available to define criteria and display specific data. Once your logical statement is defined, click “Apply filter” and data in the grid will be adjusted accordingly.



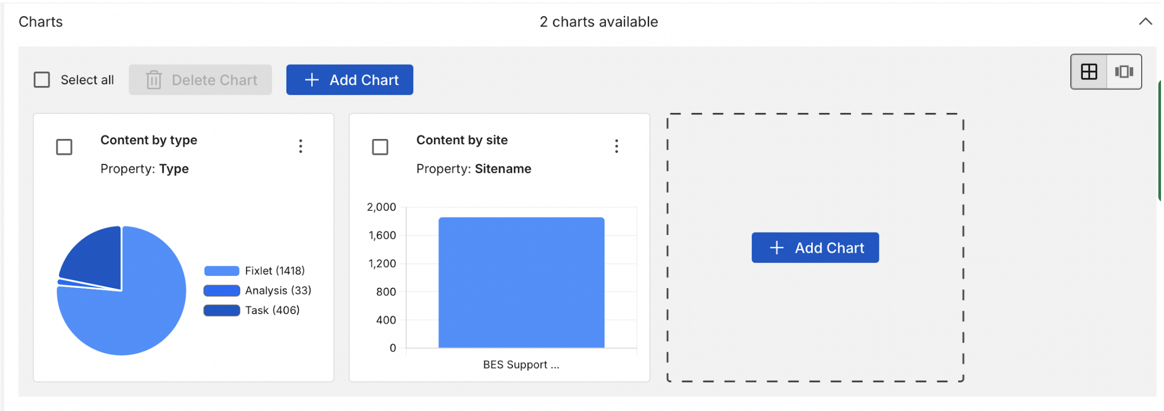
Match Type: All

Content *: Computer Property *: Agent Version Operator: contains 11.

Hint: Difference between the Filter section and the Filter button in the data grid. *While the former is used to apply complex logical expressions to the data and in the future can also be saved and shared with other users, the Filter button in the data* *grid should be used to refine the view of the data, hence will not have effect on the charts if any has been created.*

When you are done, it is possible to add a chart that gives a view of the data by a specific property. Choose a name for the chart and choose the property of the content you want to draw a chart by. At this point, you can decide what type of chart you prefer and click "Create chart".

It is possible to create multiple charts in the report.



Charts

2 charts available

Content by type

Property: **Type**

Content by site

Property: **Sitename**

Once the report looks fine to you, it can be exported in PDF and CSV formats as well as saved for future reuse.

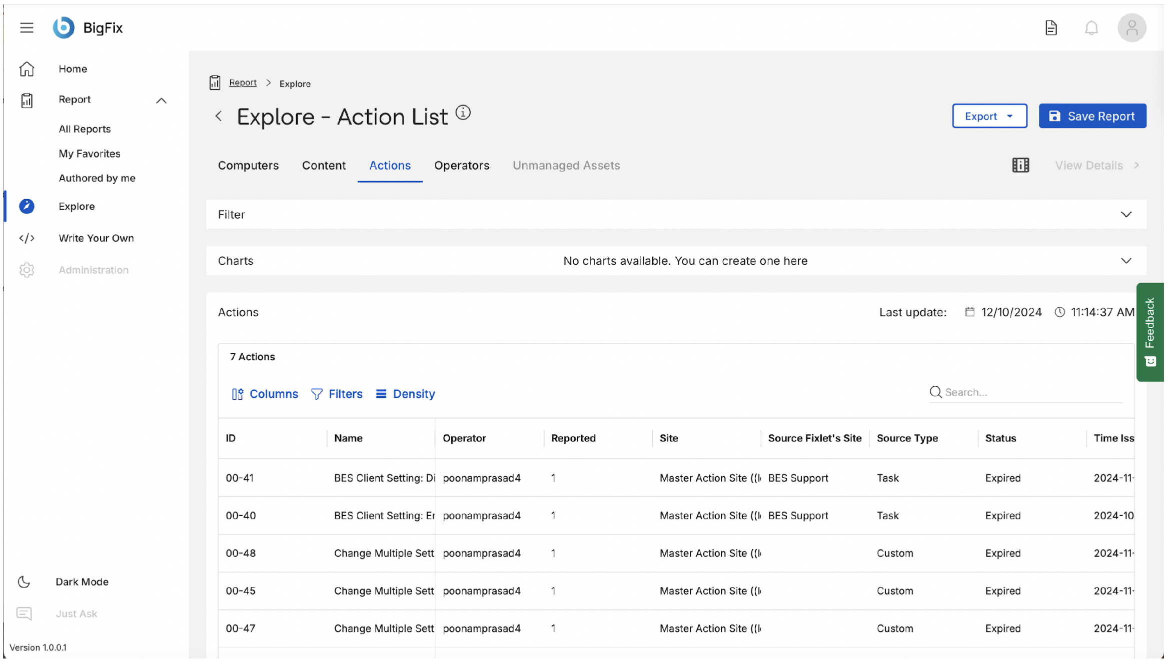
Hint: Compatibility between Web Reports and BigFix Reports
Remember that once you start making changes to a report, the same report should be managed always from the same interface

(D) I want to see all the reports I used to have in Web Reports (backward compatibility)

Permissions required: any

The user can click existing reports related to Computer, Content, Actions or Operators as well as custom report and visualize the content of the report.

Following an example of an existing report named “Actions list”



Explore - Action List

No charts available. You can create one here

Actions

Last update: 12/10/2024 11:14:37 AM

7 Actions

ID	Name	Operator	Reported	Site	Source Fixlet's Site	Source Type	Status	Time Iss
00-41	BES Client Setting: Di	poonamprasad4	1	Master Action Site ((I	BES Support	Task	Expired	2024-11-
00-40	BES Client Setting: Er	poonamprasad4	1	Master Action Site ((I	BES Support	Task	Expired	2024-10
00-48	Change Multiple Sett	poonamprasad4	1	Master Action Site ((I		Custom	Expired	2024-11-
00-45	Change Multiple Sett	poonamprasad4	1	Master Action Site ((I		Custom	Expired	2024-11-
00-47	Change Multiple Sett	poonamprasad4	1	Master Action Site ((I		Custom	Expired	2024-11-

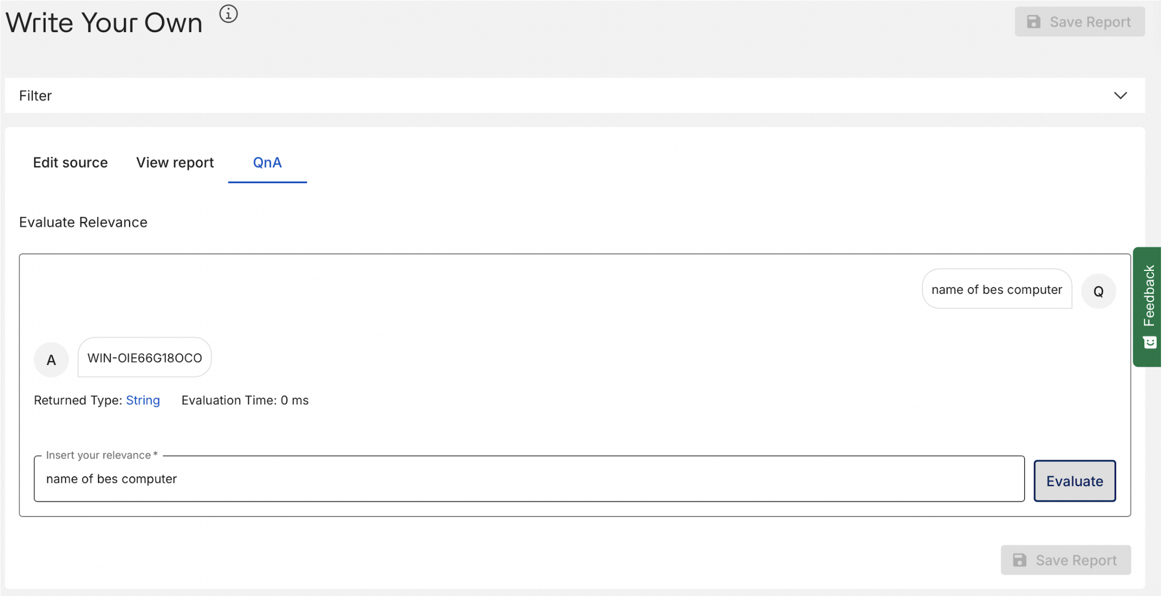
Custom reports will be rendered exactly like they are in Web Reports.

(E) I want to create a report by writing code

It is possible to create reports by writing your own code. This requires knowledge of session relevance language to retrieve data you want to display.
“Write your own” entry in the menu leads you to a page where you can insert your

code and preview how it is going to look like.

The tab QnA provides an interactive space where you can easily test your relevance before using it in the report, if needed.



Evaluate Relevance

Q: name of bes computer

A: WIN-OIE66G18OCO

Returned Type: String   Evaluation Time: 0 ms

Insert your relevance *: name of bes computer

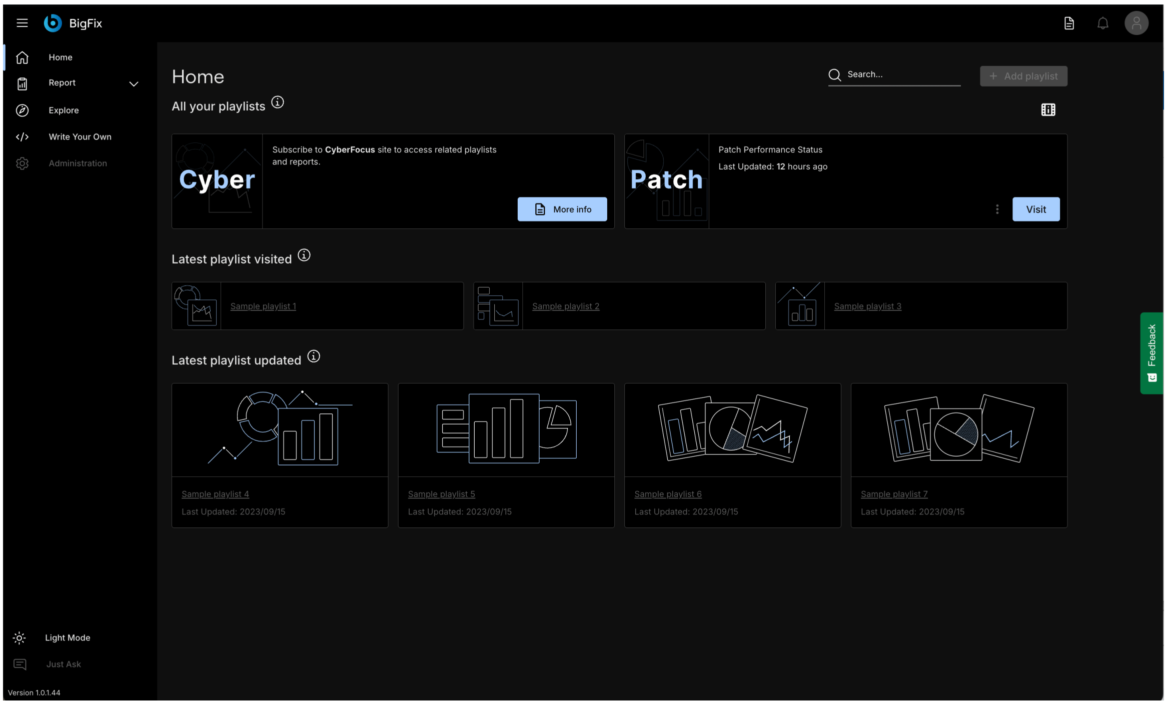
Hint: Permissions required to access edit and QNA tabs is “create content”

(F) I want to explore out of the box reports

Through the BigFix Reports interface the user has access to a number of reports provided out of the box.

Dark / Light mode

Clicking this switch on the left-hand navigation, you can switch between light and dark mode. The change will be valid throughout all the pages and can be reverted with the same button.



Home

All your playlists

Subscribe to **CyberFocus** site to access related playlists and reports.

Patch Performance Status

Last Updated: **12** hours ago

Latest playlist visited

Sample playlist 1

Sample playlist 2

Sample playlist 3

Latest playlist updated

Sample playlist 4
Last Updated: 2023/09/15

Sample playlist 5
Last Updated: 2023/09/15

Sample playlist 6
Last Updated: 2023/09/15

Sample playlist 7
Last Updated: 2023/09/15

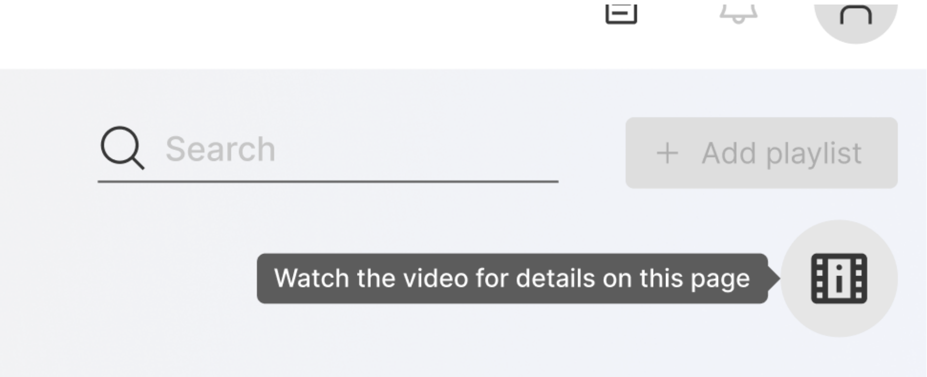
Troubleshooting

BigFix Reports does not introduce new log files, the backend leverages Web Reports engine, hence troubleshooting can be done through the usual Web Reports best practices.

> **Note:** As the new application does rely on user authentication in Web Reports, the same is also subject to timeout. If the login expires in WR, you will be asked to login again to keep on using BigFix Reports.

What’s new video

In each page you can find a link to a video to explain how to interact with the features in the page, in context.



Documentation

In the global navigation an icon will lead you to this static document. This will be the same entry point that will redirect you to the online documentation for this application.

FEEDBACK

You have the possibility to share your feedback and suggestions about the product, it will be a very short survey of paramount importance for us. We encourage you to spend just a few minutes to fill it in, you will find entry point to the survey on the right side of the page.