SOPHOS

Cybersecurity evolved.

Sophos Central Firewall Reporting FAQ

Date: May 2020

Sophos Central Firewall Reporting (CFR) Frequently Asked Questions (FAQ)

This document is a summary of the questions and answers for the Central Firewall Reporting launch. It addresses questions about the features available at GA (General Availability) and post-GA. All information is accurate as of May 2020. As is the nature of product and service development, any information given regarding the availability of features or release dates is subject to change.

Q. What is Central Firewall Reporting?

Central Firewall Reporting is Sophos' cloud-based reporting service for XG Firewalls running v18 or newer firmware. Using CFR, customers can create customized historical reports to gain insight into the applications, risks, trends, and more impacting their network.

Q. How do I get CFR?

Central Firewall Reporting is integrated into XG Firewall v18 and available on any firewall that can run this firmware.

Q. Are there different versions of CFR?

Central Firewall Reporting is available as a free version. In May 2020, we will add a "for pay" Advanced version that extends the reporting period and provides the ability to add storage capacity as needed.

Q. What will CFR Advanced offer when it launches?

When CFR Advanced becomes available, customers will be able to increase the cloud storage capacity of their syslog data in their Sophos Central account by purchasing additional capacity. Doing so will enable more syslog data to be stored for reporting purposes and will also extend the reporting period up to 365 days. Over time, the CFR Advanced license will unlock additional features as well as new pre-defined report modules.

Q. Is CFR available for Sophos SG appliances?

Central Firewall Reporting is available on Sophos XG and SG Firewalls capable of running v18 firmware.

Q. How do customers get CFR? Is there a license key?

For the free version, customers simply need to activate Central Firewall Reporting by ticking a check box in the firewall UI. No license key is required.

For the Advanced version, customers will need to purchase and activate a subscription license.

Q. How does data storage capacity work?

Syslog data is stored in the customer's Sophos Central account in the cloud where it can be retrieved as needed through the firewall to create a new report. Each firewall has a specified amount of associated storage which varies by model, with high-end 2U firewalls having the most. Customers can choose to send or not send certain log data types for cloud storage. Data is deleted using a FIFO (First In, First Out) approach.

Q. How do customers license more storage capacity?

CFR Advanced provides the option to add more storage capacity as needed through stackable 100GB licenses. Customers must purchase a minimum of a single 100GB license. The maximum storage capacity and number of 100GB licenses that can be purchased varies by firewall model.

Q. How much does it cost to add more storage capacity?

CFR Advanced is available in stackable 100GB licenses. There are three price bands based on quantity.

- 0 - 1TB at $119 per 100GB
- 1+TB - 5TB at $55 per 100GB
- 5+TB + at $50 per 100GB

As an example, three terabytes of storage would fall into the middle band at $55 per 100GB.

Q. What are the flexible customization options in CFR?

Sophos CFR provides administrators the ability to configure flexible reports with a high degree of customization. Each report table, containing dozens of column choices, allows administrators to add or remove columns of data, thereby making a report more granular, compressed, or enriched as desired. This flexibility enables administrators to define the data fields they need in their report and to see correlated data together.

Q. What are the different chart options available?

Administrators can select between a bar, pie, stacked area, and line chart for any report. In addition, the X and Y dimensions are configurable in the chart, providing a high degree of choice for deciding what to represent in a report.

Q. How flexible are the pre-defined report modules?

Reports are structured around specific modules such as Application Usage, Web Usage, etc. Each of the reports can be further customized by changing data fields in the table and charts and applying filters to the hundreds of data fields. The flexible report table and charts allow users to customize each report and create a library of hundreds of variations from any report. Each report provides multiple charting options, enabling administrators to visualize data and trends for their specific use case. As an example, the Application Bandwidth report uses a stacked area chart showing bandwidth consumption over a defined period.

Q. What happens when a customer upgrades from the free version of CFR to Advanced?

Upgrading from the free version to CFR Advanced will enable more syslog data to be stored for reporting purposes and extend the reporting period up to 365 days. In addition, new features as well as new pre-defined report modules will become available over time.

Q. If a customer stops using either version, what happens to the log data at any point in time?

The syslog data is stored in the customer's Sophos Central account in the cloud. Data is added and removed on a FIFO (First In, First Out) basis. Therefore, once the storage capacity maximum is reached, newly-added data will replace the oldest data.

Q. Can customers utilize third-party reporting applications using the stored data?

CFR will not function as a log forwarder. Organizations that need to store their log data in a third-party SIEM or log collector in addition to Sophos Central can configure their XG firewall to send data to multiple locations in parallel (e.g. a local SIEM and Sophos Central).

Q. What happens if the storage capacity for the firewall is exceeded?

Data is deleted using a FIFO approach. When a given firewall consumes all its allocated storage, data is rotated according to FIFO. The expiry date is dictated by the rate at which the firewall sends data to Sophos Central. CFR Advanced customers may purchase more storage capacity up to the firewall's limit.

Q. How far back does the historical reporting go?

The free version enables reporting for up to seven days based on the amount of log data generated and the firewall's storage capacity. The Advanced version enables a longer period of reporting up to one year. CFR Advanced customers can expand or shrink the storage allocated to a given device at any time. Doing so will either expand or reduce the duration for which the old log data is available.

Q. Will CFR be supported on XG Firewall software, virtual, and cloud instances?

Yes. CFR is available on all XG Firewall platforms that can run v18 firmware.

Q. What is the plan for adding more features and pre-defined reports?

We are taking a rolling approach with regard to adding new features and reports. Because CFR is cloud-based, customers will not need to update/upgrade the firewall firmware to take advantage of new features when they are introduced.

Some features and reports will be phased in across both the Free and Advanced versions while others will be available only to customers who have CFR Advanced. As the new features and reports are rolled out, we will communicate their availability and on which CFR version(s) they will be available.

Q. What is the Report Dashboard?

The Report Dashboard is an at-a-glance view from the XG Firewall for network operational health, policy control events, and all security-driven events. Sometimes administrators just need to get a quick glance of the previous 24 hours of events without having to dive into a more detailed report. The Report Dashboard surfaces the top network, security, and policy-driven events. From the dashboard, administrators can quickly pivot into a full report for a more detailed analysis.

Q. Is reporting available via Sophos Central?

Yes. Customers can create reports either through the firewall or their Sophos Central account.

Q. Is the report data “real-time” or is there a lag for visualizing and reporting on the data?

There is a slight delay while the syslog data is retrieved from the customer’s Sophos Central account in the cloud, so it could potentially take up to several minutes to generate the desired report in some instances.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

191126 EN (PMM_BLH)

SOPHOS