

IBM Security QRadar
Version 7.1.0 (MR1)

*Enabling Payload Indexing For Quick
Filtering Technical Note*

IBM

Note: Before using this information and the product that it supports, read the information in [Notices and Trademarks](#) on [page 5](#).

CONTENTS

1	PAYLOAD INDEXING	
	Enabling Payload Indexing	3
	Configuring the Payload Index Retention Period	4
	Troubleshooting	4

A	NOTICES AND TRADEMARKS	
	Notices	5
	Trademarks	7

1

PAYLOAD INDEXING

The Quick Filter feature in both the **Log Activity** and **Network Activity** tabs enables you to search event and flow payloads using a text string. Where Quick Filter searches take an extended time period, you can optimize the search by enabling a payload index on the Quick Filter property.

Enabling payload indexing increases disk storage requirements and could decrease system performance. We recommend that you only enable payload indexing if the event and flow processors in your deployment are:

- At no greater than 70% disk utilization
- At no greater than 70% of the maximum Events Per Second (EPS) or Flows Per Interface (FPI) rating

Unless otherwise noted, all references to QRadar SIEM refer to QRadar SIEM, IBM Security QRadar Log Manager, and IBM Security QRadar Network Anomaly Detection. References to flows do not apply to QRadar Log Manager.

This section includes the following topics:

- [Enabling Payload Indexing](#)
- [Configuring the Payload Index Retention Period](#)
- [Troubleshooting](#)

Enabling Payload Indexing

To enable payload indexing on the Quick Filter property:

- Step 1** Log in to QRadar SIEM.
- Step 2** Click the **Admin** tab.
- Step 3** On the navigation menu, click **System Configuration**.
- Step 4** Click the **Index Management** icon.
The Index Management window is displayed.
- Step 5** In the **Quick Search** field, type **Quick Filter**.
The Quick Filter property is displayed for events and flows.
- Step 6** Select the **Quick Filter** property you want to index.

You can identify the event and flow Quick Filter properties using the value in the **Database** column.

Step 7 On the toolbar, Click **Enable Index**.

A green dot is displayed to indicate the payload index is enabled.

NOTE

You can also right-click the Quick Filter property and select **Enable Index**.

Step 8 Click **Save**.

A confirmation window is displayed.

Step 9 Click **OK**.

The selected Quick Filter properties are now indexed. In lists that include event or flow properties, indexed property names are appended with the following text:

[Indexed].

Configuring the Payload Index Retention Period

You can configure the time period to store Quick Filter payload indexes. By default, payload indexes are retained for one week. The minimum retention period is one day and the maximum is two years.

To configure the payload index retention period:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

The System Configuration pane is displayed.

Step 3 Click the **System Settings** icon.

The System Settings window is displayed.

Step 4 In the Database Settings pane, select a retention time period from the **Payload Index Retention** list box.

Step 5 Click **Save**.

Step 6 Close the System Settings window.

Step 7 On the **Admin** tab menu, click **Deploy Changes**.

Your payload index retention period is now configured.

Troubleshooting

When you enable payload indexing, the following warning message may be displayed:

```
Payload indexing is disabled because we have detected that one or more hosts in your deployment will experience performance degradation after enabling payload indexing. The performance degradation could extend to loss of events and/or flows.
```

If this message is displayed, contact Customer Support for assistance preparing your systems to support payload indexing.

A

NOTICES AND TRADEMARKS

What's in this appendix:

- [Notices](#)
- [Trademarks](#)

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

Enabling Payload Indexing for Quick Filtering

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

