IBM Security QRadar
Version 7.2.1

Using the QID Map

Note: Before using this information and the product that it supports, read the information in Notices and trademarks on page 9.

CONTENTS

1 MANAGING QRADAR USER-DEFINED QID MAP ENTRIES

The QRadar® Identifier (QID) map provides the association or mapping of an external device event to a unique identifier. Use the QID map utility to create, export, import, or modify user-defined QID map entries.

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

Creating a QID map entry

Use the QID map utility to create a QID map entry.

About this task

The utility provides the following options:

```
qidmap_cli.sh [-l|-c|-m|-i[-f <filename>]|-e[-f <filename>]|-d]
```

The following table describes the utility options:

Table 1-1 QID Map utility options

Parameter	Description
-l	Lists the low-level category.
-c	Creates a new QID map entry.
-m	Modifies an existing user-defined QID map entry.
-i	Imports QID map entries.
-e	Exports existing user-defined QID map entries.
-f <filename>	If you include the -i or -e option, type a filename to import or export QID map entries.
-d	If you include the -i or -e option, type a delimiter for the import or export file. The default is a comma.
-h	Display the help options.

Procedure

Step 1 Using SSH, log in to QRadar as the root user.

Step 2 To locate the appropriate low-level category for the QID map entry you want to create, type the following command:

```
/opt/qradar/bin/qidmap_cli.sh -l
```

If you want to search for a particular low-level category, you can use the grep command to refine the results:

```
/opt/qradar/bin/qidmap_cli.sh -l | grep <text>
```

Step 3 Type the following command:

```
qidmap_cli.sh -c --qname <name> --qdescription <description>
--severity <severity> --lowlevelcategoryid <ID>
```

The following table provides the utility options:

Table 1-2 Create QID Map utility options

Options	Description
-c	Creates a new QID map entry.
--qname <name>	Type the name you want to associate with this QID map entry. The name can be up to 255 characters in length, with no spaces.
--qdescription <description>	Type a description for this QID map entry. The description can be up to 2048 characters in length with no spaces.
--severity <severity>	Type the severity level you want to assign to this QID map entry. The valid range is 0 to 10.
--lowlevelcategoryid <ID>	Type the low-level category ID you want to assign to this QID map entry. For more information on low-level categories, see the *Administration Guide* for your product.

Modifying a QID map entry

You can modify an existing user-defined QID map entry.

Procedure

Step 1 Using SSH, log in to QRadar as the root user.

Step 2 To modify a QID Map entry, type the following command:

```
qidmap_cli.sh -m --qid<QID> --qname <name> --qdescription
<description> --severity <severity>
```

The following table provides the utility options:

Table 1-3 Modify QID Map utility options

Options	Description
-m	Modifies an existing user-defined QID map entry.
--qid<QID>	Type the QID that you want to modify.
--qname <name>	Type the name you want to associate with this QID map entry. The name can be up to 255 characters in length with no spaces.
--qdescription <description>	Type a description for this QID map entry. The description can be up to 2048 characters in length with no spaces.
--severity <severity>	Type the severity level you want to assign to this QID map entry. The valid range is 0 to 10.

Importing QID map entries

You can import QID map entries from a text file by using the QID map utility.

Procedure

Step 1 Create a .txt file that includes the user-defined QID map entries you want to import. Ensure that each entry in the file is separated using a comma. Choose one of the following options:

- To import a new list of user-defined QID map entries, create the file using the following format for each entry:

  ,<name>,<description>,<severity>,<category>

  For example:

  ,buffer,buffer_QID,7,18401

  ,malware,malware_misc,8,18403

- To import an existing list of user-defined QID map entries, create the file using the following format for each entry:

  <qid>,<name>,<description>,<severity>

  For example,

  2000002,buffer,buffer_QID,7

  2000001,malware,malware_misc

The following table provides the import options:

Table 1-4 Import QID Map utility options

Options	Description
<qid>	This option is required if you want to import an existing exported list of QID entries. Type the existing QID for the entry. If you want to import new QID entries, do not use this option. The QID map utility assigns an identifier (QID) for each entry in the file.
--qname <name>	Type the name you want to associate with this QID map entry. The name can be up to 255 characters in length.
--qdescription <description>	Type a description for this QID map entry. The description can be up to 2048 characters in length.
--severity <severity>	Type the severity level you want to assign to this QID map entry. The valid range is 0 to 10.
--lowlevelcategoryid <ID>	Type the low-level category ID you want to assign to this QID map entry. For more information on low-level categories, see the *IBM Security QRadar SIEM Administration Guide.* This option is only necessary if you want to import a new list of QID entries. Type the existing QID for the entry.

Step 2 Save and exit the file.

Step 3 Using SSH, log in to QRadar SIEM as the root user.

Step 4 Import the QID map file, by typing the following command:

```
/opt/qradar/bin/qidmap_cli.sh -i -f <filename.txt>
```

Where **<filename>** is the directory path and name of the file that contains the QID map entries. If any of the entries in the file cause an error, none of the entries in the file are enforced.

Exporting QID map entries

You can export user-defined QID map entries to a text file by using the QID map utility.

Procedure

Step 1 Using SSH, log in to QRadar as the root user.

Step 2 To export the QID map file, type the following command:

`/opt/qradar/bin/qidmap_cli.sh -e -f <filename.txt>`

Where **`<filename>`** is the directory path and name of the file you want to contain your QID map entries.

A NOTICES AND TRADEMARKS

What's in this appendix:

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:

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 is for planning purposes only. The information herein is subject to change before the products described become available.

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 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*.