

TECHNICAL NOTE

MANAGING USER-DEFINED QID MAP ENTRIES

OCTOBER 2009

The STRM Identifier (QID) map provides the association or mapping of an event of an external device to a STRM unique identifier (QID).

You can use the QID map utility to create, export, import, or modify user-defined QID map entries. This document provides information on managing QID map entries including:

- [Using the Utility](#)
- [Creating a QID Map Entry](#)
- [Modifying a QID Map Entry](#)
- [Importing QID Map Entries](#)
- [Exporting QID Map Entries](#)

Using the Utility

The utility provides the following options:

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

The following table provides the utility options:

Table 1 QID Map Utility Options

Options	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 specify the -i or -e option, allows you to specify a file name to import or export QID map entries.
-d	If you specify the -i or -e option, allows you to specify a delimiter for the import or export file. The default is a comma.
-h	Display the help options.

Creating a QID Map Entry

To create a QID map entry:

Step 1 Log in to STRM, as root.

Step 2 Locate the appropriate low-level category for the QID map entry you want to create:

```
/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>
```

The list of low-level categories appears.

Step 3 Enter the following command:

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

The following table provides the utility options:

Table 2 Create QID Map Utility Options

Options	Description
-c	Creates a new QID map entry.
--qname <name>	Specify 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>	Specify a description for this QID map entry. The description can be up to 2048 characters in length with no spaces.
--severity <severity>	Specify the severity level you wish to assign to this QID map entry. The valid range is 0 to 10.
--lowlevelcategoryid <ID>	Specify the low-level category ID you wish to assign to this QID map entry. For more information on low-level categories, see the <i>Event Category Correlation Reference Guide</i> .

Modifying a QID Map Entry

To modify an existing user-defined QID map entry:

Step 1 Log in to STRM, as root.

Step 2 Enter the following command:

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

The following table provides the utility options:

Table 3 Modify QID Map Utility Options

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

Importing QID Map Entries

Using the QID map utility, you can import QID map entries from a .txt file.

To import QID map entries:

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

a If you want 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
```

b If you want 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 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. Specify the existing QID for the entry. If you wish 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>	Specify the name you want to associate with this QID map entry. The name can be up to 255 characters in length.
--qdescription <description>	Specify a description for this QID map entry. The description can be up to 2048 characters in length.
--severity <severity>	Specify the severity level you wish to assign to this QID map entry. The valid range is 0 to 10.
--lowlevelcategoryid <ID>	Specify the low-level category ID you wish to assign to this QID map entry. For more information on low-level categories, see the <i>Event Category Correlation Reference Guide</i> . This option is only necessary if you want to import a new list of QID entries. Specify the existing QID for the entry.

Step 2 Save and exit the file.

Step 3 Log in to STRM, as root.

Step 4 Import the QID map file:

```
/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

Using the QID map utility, you can export user-defined QID map entries to a .txt file.

To export user-defined QID map entries:

Step 1 Log in to STRM, as root.

Step 2 Export the QID map file:

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

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

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Published: 2009-10-12