

IBM Security QRadar
Version 7.1.0 (MR1)

Mapping Packeteer Technical Note



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

CONTENTS

1	MAPPING PACKETEER APPLICATIONS	
	Mapping a Packeteer Class ID	3

A	NOTICES AND TRADEMARKS	
	Notices	5
	Trademarks	7

1

MAPPING PACKETEER APPLICATIONS

Packeteer devices collect, aggregate, and store network performance data. After you configure an external flow source for Packeteer, you can send flow information from a Packeteer device to QRadar SIEM. This allows QRadar SIEM to:

- Support packeteer FDR records.
- Classify, store, display, report, and apply NBAD to Packeteer data.
- Map standard Packeteer supported applications.
- Support any custom applications.

This technical note applies to systems running QRadar SIEM 6.1 and above. Unless otherwise noted, all references to QRadar SIEM refer to QRadar SIEM and IBM Security QRadar Network Anomaly Detection. References to flows do not apply to QRadar Log Manager.

When you create a new class ID in your Packeteer device, you must map this ID to a QRadar SIEM application ID. This allows QRadar SIEM to process the new class ID as a QRadar SIEM application ID. This document provides procedures for mapping a Packeteer class ID to a QRadar SIEM application ID.

NOTE

For more information on QRadar SIEM application IDs, see the *IBM Security QRadar SIEM Application Configuration Guide*.

Mapping a Packeteer Class ID

To map a Packeteer class ID to a QRadar SIEM application ID:

- Step 1** Create the new class ID in the Packeteer device.
For more information on creating a new class ID, see your Packeteer documentation.
- Step 2** Using SSH, log in to QRadar SIEM as root user:
Username: **root**
Password: **<password>**
- Step 3** Open the following file:
`/opt/qradar/conf/packeteer.conf`

Step 4 At the end of the file, add a line for each new mapping you want to create in the following format:

```
<class ID>,<application ID>
```

Where:

<class ID> is the Packeteer class ID.

<application ID> is the associated QRadar SIEM application ID.

Step 5 Save and exit the file.

Step 6 Log in to the QRadar SIEM interface.

```
https://<IP Address>
```

Where <IP Address> is the IP address of the QRadar SIEM system.

Username: `admin`

Password: <root password>

Where <root password> is the password assigned to QRadar SIEM during the installation process.

Step 7 Click the **Admin** tab.

Step 8 On the navigation menu, click **System Configuration**.

The System Configuration pane is displayed.

Step 9 Click the **System and License Management** icon.

The System and License Management window is displayed.

Step 10 Select the system you want to restart.

Step 11 From the **Actions** menu, select **Restart System**.

QRadar SIEM restarts.

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:

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>.

