Gigamon®

Application Metadata Intelligence with QRadar Integration Guide

Document Version: 1.0

(See *Change Notes* for document updates)

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and provide a link to the Change Notes table, which describes the updates.

Document Version	Date Updated	Change Notes
1.0	17-03-2026	The original release of this document.

Contents

Change Notes 1
Application Intelligence Solution Integration with QRadar 3
Prerequisites 4
Configure QRadar by using the web UI (admin) 5
Configure QFlow IPFIX encoding 5
Configure QRadar UI-Flows 5
Install the Gigamon IPFIX Metadata application 5
Configure QRadar details in GigaVUE-FM and Deploy 6
Verify the Integration 6
Visualize the Dashboards in QRadar 6

Application Intelligence Solution Integration with QRadar

This guide provides step-by-step instructions for monitoring application metadata from Gigamon using QRadar.

Note:

- *The guide is intended for customer deployments and assumes familiarity with basic GigaVUE-FM and QRadar administration.*
- *The integration flow outlined in this guide is based on GigaVUE-FM version 6.12 and QRadar 7.5.11. Menu labels and UI layouts may change slightly across releases. Always refer to the latest GigaVUE Documentation Library and QRadar Documentation for UI details.*

Prerequisites

Before you start with the integration, ensure the following are in place:

- AMI solutions are deployed. For instructions, refer to:
  - Create Application Metadata Intelligence for Physical Environment
  - Create Application Metadata Intelligence for Virtual Environment
- QRadar credentials:
  - UI: Login as the admin user.
  - CLI: SSH access to the QRadar console as root.
- Ensure that when working with QRadar:
  - UI actions are done as admin.
  - CLI changes are done as root.
- Gigamon QRadar IPFIX Record template (JSON) for GigaVUE-FM:
  Use the QRadar Template referenced from the deployment guide and upload it into GigaVUE-FM when configuring the IPFIX record.

Update the Gigamon Private Enterprise Number (PEN) name

Perform these steps on the QRadar console as root.

1. Update the Gigamon PEN name. Edit the PEN file:
   vi /opt/qradar/conf/iana-pen.conf
2. Locate PEN ID 26866 and change the name from "Gigamon Systems LLC" to "Gigamon".
3. Save the file.

Add the Gigamon private IPFIX elements.

Edit the IPFIX fields file:
vi /opt/qradar/conf/IPFIXFields.conf

1. Append the provided Gigamon IPFIX field definitions to the end of the file.
2. Save the file.

Configure QRadar by using the web UI (admin)

To create and configure QRadar :

1. Log in to the QRadar UI as admin. Go to **Admin** > **System and License Management**.
2. Select the console host to edit. Ensure the Display is set to **Systems**, then click the **Display Systems** drop-down.
3. Select Edit the host and click on **Component Management** box.
4. In the component configuration configure the following details:
    a. Maximum Content Capture value is 5120.
    b. Maximum Data Capture value 1024.
    c. Flow buffer size value 100,000.
5. Click **Save** once edited.

Configure QFlow IPFIX encoding

To create and configure QRadar:

1. Select the **System settings**, in the **QFlow settings for IPFIX Additional Field Encoding**, select TLV and Payload.
2. Click **Save** and Close, in the **Admin** page click **Deploy Changes**.

Configure QRadar UI-Flows

To create and configure QRadar :

1. In the Flows section > Flows Sources.
2. Select the default_netflow and click **Edit** option.
3. Configure following information:
    a. Monitoring Port:2055
    b. Linking Protocol:UDP.
4. Click **Save** and Close.

Install the Gigamon IPFIX Metadata application

To create and configure QRadar :

1. Download the Gigamon IPFIX Metadata application for QRadar from IBM Application Exchange.
2. In the QRadar UI, go to **Admin > Extensions Management**. In the Extension Management window, click on **Add** to add the Extensions.
3. In the New Extension Management window, click **Browse** in the window and select the Gigamon AMI application zip file.
4. Click **Add** and save, in the **Admin** page click **Deploy Changes**.

Note:

After completing all the preceding steps, restart the service to apply the changes. From the CLI, run the following command:
service host context restart

Configure QRadar details in GigaVUE-FM and Deploy

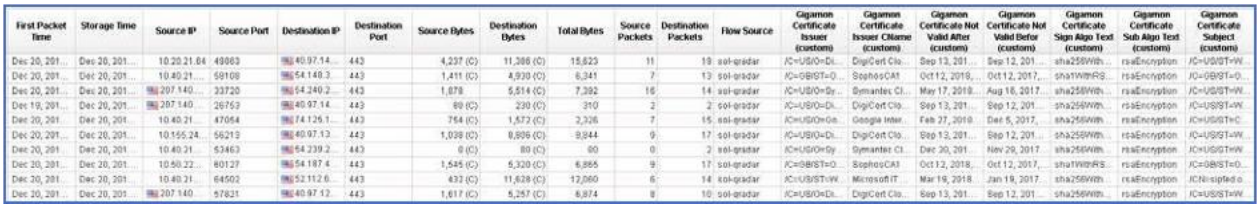
To set up QRadar Template in GigaVUE-FM:

1. Log into GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows**, and select your platform.
2. Open a monitoring session that contains the AMI node and open **Traffic Processing**.
3. Select the AMI node in the Monitoring Session to open its configuration panel.
4. In the AMI Node, click on **Menu** > **Details**. Open **Exporters Section**.
5. In the Exporters section, click on the **Actions** > **Add Exporter**, and then provide an **Exporter name**.
6. In the **Template**, click on **Apply Template** and select **QRadar Template**. (Ensure the QRadar template is applied in AMI Exporter). Click **save** to apply the configuration.
7. Add a New Tunnel:
    a. Alias: Provide a name.
    b. Type: UDP
    c. Destination Address: IP Address
    d. Destination L4 Port: 2055
8. Click **Save** and return to the Canvas.
9. Connect the AMI to the New Tunnel and click **Actions > Deploy**.

Verify the Integration

To verify if the integration is successful

1. Log in to your QRadar account.
2. In the Menu click on the **Network Activity** to observe the traffic flow.

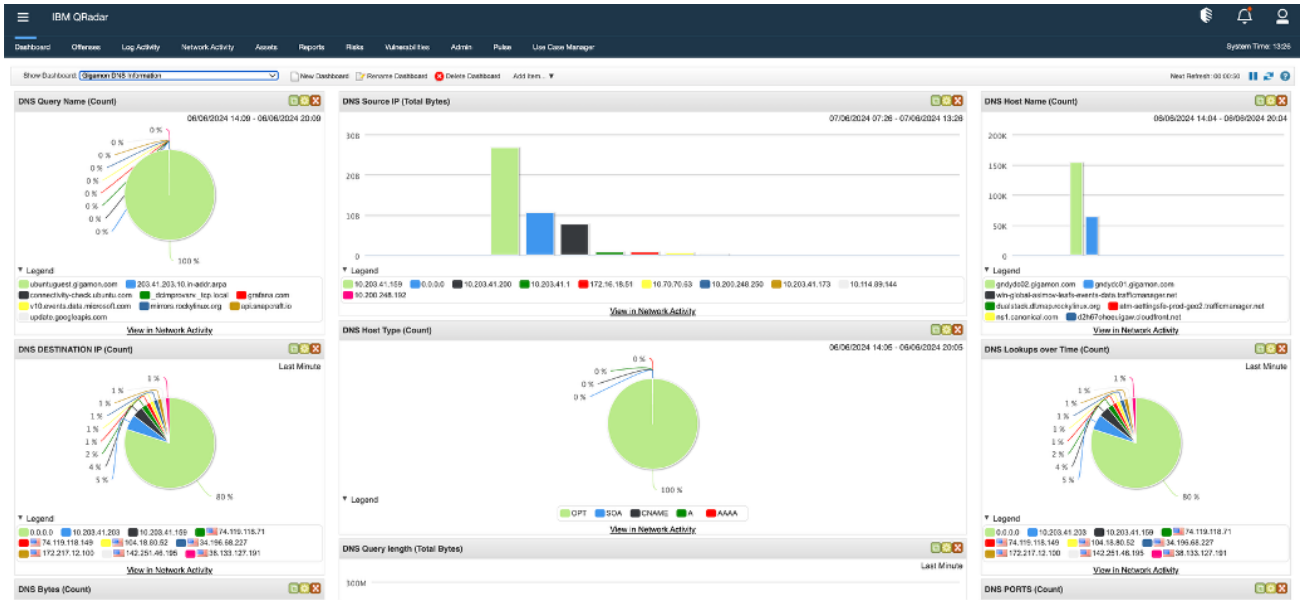


First Packet Time	Storage Time	Source IP	Source Port	Destination IP	Destination Port	Source Bytes	Destination Bytes	Total Bytes	Source Packets	Destination Packets	Flow Source	Gigamon Certificate Issuer (custom)	Gigamon Certificate Issuer CName (custom)	Gigamon Certificate Not Valid After (custom)	Gigamon Certificate Not Valid Befor (custom)	Gigamon Certificate Sign Algo Text (custom)	Gigamon Certificate Sub Algo Text (custom)	Gigamon Certificate Subject (custom)
Dec 20, 201...	Dec 20, 201...	10.20.21.84	49083	40.97.14...	443	4,237 (C)	11,386 (C)	15,623	11	19	sol-gradar	/C=US/O=Di...	DigiCert Clo...	Sep 13, 201...	Sep 12, 201...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 20, 201...	Dec 20, 201...	10.40.21....	59109	54.148.3...	443	1,411 (C)	4,930 (C)	6,341	7	13	sol-gradar	/C=GB/ST=O...	SophosCA1	Oct 12, 2019,...	Oct 12, 2017,...	sha1WithRS...	rsaEncryption	/O=GB/ST=O...
Dec 20, 201...	Dec 20, 201...	207.140....	33720	54.240.2...	443	1,878	5,514 (C)	7,392	16	14	sol-gradar	/C=US/O=Sy...	Symantec Cl...	May 17, 2019...	Aug 16, 2017...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 19, 201...	Dec 20, 201...	207.140....	26753	40.97.14...	443	80 (C)	230 (C)	310	2	2	sol-gradar	/C=US/O=Di...	DigiCert Clo...	Sep 13, 201...	Sep 12, 201...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 20, 201...	Dec 20, 201...	10.40.21....	47064	74.125.1...	443	764 (C)	1,572 (C)	2,336	7	15	sol-gradar	/C=US/O=Go...	Google Inter...	Feb 27, 2019...	Dec 5, 2017,...	sha256With...	rsaEncryption	/C=US/ST=C...
Dec 20, 201...	Dec 20, 201...	10.155.24...	56213	40.97.13...	443	1,039 (C)	8,805 (C)	9,844	9	17	sol-gradar	/C=US/O=Di...	DigiCert Clo...	Sep 13, 201...	Sep 12, 201...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 20, 201...	Dec 20, 201...	10.40.21....	53463	54.239.2...	443	0 (C)	80 (C)	80	0	2	sol-gradar	/C=US/O=Sy...	Symantec Cl...	Dec 30, 201...	Nov 29, 2017...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 20, 201...	Dec 20, 201...	10.50.22....	60127	54.187.4...	443	1,545 (C)	5,320 (C)	6,865	9	17	sol-gradar	/C=GB/ST=O...	SophosCA3	Oct 12, 2018,...	Oct 12, 2017,...	sha1WithRS...	rsaEncryption	/C=GB/ST=O...
Dec 20, 201...	Dec 20, 201...	10.40.21....	64502	52.112.6...	443	432 (C)	11,628 (C)	12,060	6	14	sol-gradar	/C=US/ST=W...	Microsoft IT...	Mar 19, 2018...	Jan 19, 2017...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 20, 201...	Dec 20, 201...	207.140....	57831	40.97.12...	443	1,617 (C)	5,257 (C)	6,874	9	10	sol-gradar	/C=US/O=Di...	DigiCert Clo...	Sep 13, 201...	Sep 12, 201...	sha256With...	rsaEncryption	/C=US/ST=W...

Visualize the Dashboards in QRadar

To create and configure QRadar :

1. Log in to your QRadar account.
2. Click on **Dashboard** in the menu, in the **Show Dashboards** click on the drop-down to view the specific dashboard.



Copyright 2026 Gigamon Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. No part of this publication may be reproduced, transcribed, translated into any language, stored in a retrieval system, or transmitted in any form or any means without the written permission of Gigamon Inc.

Trademark Attributions

Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners.

Gigamon Inc. 3300 Olcott Street

Santa Clara, CA 95054 408.831.4000

© 2026 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.