IBM Security QRadar
Version 7.2.6

Upgrade Guide

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

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to upgrading QRadar software

Information about upgrading IBM® Security QRadar® applies to IBM Security QRadar SIEM, IBM Security QRadar Log Manager products.

Intended audience

System administrators who are responsible for upgrading IBM Security QRadar systems must be familiar with network security concepts and device configurations.

Technical documentation

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Chapter 1. Preparation for the upgrade

To successfully upgrade IBM Security QRadar systems, ensure that you know your upgrade path, especially if you upgrade from older versions that require intermediate steps. You must also review the software, hardware, and high-availability requirements.

Important: When you upgrade to QRadar V7.2.6 and later releases, the SSH keys on every managed host are replaced. If you are connecting to or from a QRadar managed host and you are using key-based authentication, do not remove or alter the SSH keys. Removing or altering the keys might disrupt communication between the QRadar Console and the managed hosts, which can result in lost data.

Software version requirements for upgrades

To ensure that IBM Security QRadar upgrades without errors, ensure that you use only the supported versions of QRadar software.

Ensure that the following software requirements are met:

- QRadar version 7.2.4983526 or later must be installed.

  You can check the software version in the software by clicking **Help** > **About**.

  Important: Software versions for all IBM Security QRadar appliances in a deployment must be same version and fix level. Deployments that use different QRadar versions of software are not supported.

Upgrade paths

There are a number of upgrade paths to get to the most current version of IBM Security QRadar. The upgrade path depends on the version of QRadar that is installed.

Applying fix packs before you upgrade

Before you upgrade, you can apply fixes (fix pack) to your existing software. Download the fix pack from IBM Fix Central (www.ibm.com/support/fixcentral) and follow the instructions in the release notes document to install it.

QRadar is pre-configured for automatic, weekly updates. You can view the pending updates in the Updates window on the **Admin tab**.

Single step and multiple step upgrade paths

For some QRadar software versions, you can upgrade directly to the most current QRadar version. To upgrade to QRadar version V7.2.6 in one step, you must have QRadar version 7.2.4.983526 or later installed. When you upgrade from QRadar version 7.2.4.983526 or later, pre-tests identify any potential upgrade issues, and you are returned to the software level that you started from if you encounter upgrade errors. Also, in high-availability deployments, the secondary host upgrades before the primary to maximize up-time.

For older versions of QRadar, you might be required to upgrade to an interim version before you upgrade to the most current version of QRadar.

Use the following table to help you determine your upgrade path and note any special considerations.

Table 1. Supported upgrade paths for QRadar products.

Current® version	Step 1	Step 2	Step 3
7.1 (MR2) (7.1.0.501605) or later	7.2.4 (SFS)		
7.1 GA to 7.1 (MR1) Patch 3 (7.1.0.380596 to 7.1.0.495292)	7.1 MR2 Patch 2 (7.1.0.599086) (SFS)	7.2.4 (SFS)	
7.0 (MR5) to 7.0 (MR5) Patch 7 (7.0.0.301503 to 7.0.0.672904)	7.1 MR2 Patch 2 (7.1.0.599086) (ISO)	7.2.4 (SFS)	
7.0 GA to 7.0 MR4 Patch 2 (7.0.0.167618 to 7.0.0.276729)	7.0 MR5 (7.0.0.301503) (SFS)	7.1 MR2, (7.1.0.599086) (ISO)	7.2.4 (SFS)

Memory and disk space requirements

Before you upgrade, ensure that IBM Security QRadar meets the minimum or suggested memory and disk space requirements.

QRadar memory requirements

The following table describes the minimum and suggested memory requirements for QRadar appliances. The minimum memory requirement defines the amount of memory that is required by the software features. The suggested memory requirements include the amount of memory that is required by the current software features and extra memory for possible future capabilities. Appliances that have less than the suggested appliance memory might experience performance issues during periods of excessive event and flow traffic.

Table 2. Minimum and optional memory requirements for QRadar appliances

Appliance	Minimum memory requirement	Suggested memory requirement
QFlow Collector 1201	6 GB	6 GB
QFlow Collector 1202	6 GB	6 GB
QFlow Collector Virtual 1299 without QRadar Vulnerability Scanner	2 GB	2 GB
QFlow Collector Virtual 1299 with QRadar Vulnerability Scanner	6 GB	6 GB
QFlow Collector 1301	6 GB	6 GB
QFlow Collector 1310	6 GB	6 GB
QRadar Event Collector 1501	12 GB	16 GB
QRadar Event Collector Virtual 1599	12 GB	16 GB
QRadar Event Processor 1601	12 GB	48 GB
QRadar Event Processor 1605	12 GB	48 GB
QRadar Event Processor 1624	64 GB	64 GB

Table 2. Minimum and optional memory requirements for QRadar appliances (continued)

Appliance	Minimum memory requirement	Suggested memory requirement
QRadar Event Processor 1628	128 GB	128 GB
QRadar Event Processor Virtual 1699	12 GB	48 GB
QRadar Flow Processor 1701	12 GB	48 GB
QRadar Flow Processor 1705	12 GB	48 GB
QRadar Flow Processor 1724	64 GB	64 GB
QRadar Flow Processor 1728	128 GB	128 GB
QRadar Flow Processor Virtual 1799	12 GB	48 GB
QRadar Event and Flow Processor 1805	12 GB	48 GB
QRadar Event and Flow Processor 1824	64 GB	64 GB
QRadar Event and Flow Processor 1828	128 GB	128 GB
QRadar SIEM 2100	24 GB	24 GB
QRadar SIEM 2100 Light	24 GB	24 GB
QRadar SIEM 3100	24 GB	48 GB
QRadar SIEM 3105	24 GB	48 GB
QRadar SIEM 3124	64 GB	64 GB
QRadar SIEM 3128	128 GB	128 GB
QRadar SIEM Virtual 3199	24 GB	48 GB
QRadar Log Manager 1605	12 GB	48 GB
QRadar Log Manager 1624	64 GB	64 GB
QRadar Log Manager 1628	128 GB	128 GB
QRadar Log Manager 2100	24 GB	24 GB
QRadar Log Manager 3105	24 GB	48 GB
QRadar Log Manager 3124	64 GB	64 GB
QRadar Log Manager 3128	128 GB	128 GB
QRadar Log Manager 3199	24 GB	48 GB

Other memory requirements

If the following conditions are met, extra memory requirements might be required:

- If you plan to enable payload indexing, your system requires a minimum of 24 GB of memory. However, 48 GB of memory is suggested.
- If you install QRadar software on your own hardware, your system requires a minimum of 24 GB of memory.

Disk space requirements

The following table describes the minimum requirements for free disk space:

Table 3. Disk space requirements for QRadar

Partition	Free space requirement
/	3 GB or 10 GB [1]
/store	4 GB
/var/log	500 MB
/store/tmp	800 MB
[1]If your appliance has less than 8 GB of available swap space or 5 GB of memory, the root (/) partition requires 10 GB of drive space. Otherwise, appliances require a minimum of 3 GB of disk space on the root partition.	

Restriction: If your IBM Security QRadar QFlow Collector appliances have less than an 80 GB of available disk space, you must install the most current software version. For more information, see the *Installation Guide* for your product.

The upgrade pretest determines whether a partition includes enough free space to complete an upgrade. Before you can upgrade, you must free up sufficient disk space on the partition that is defined in the pretest error message.

Supported web browsers

For the features in IBM Security QRadar products to work properly, you must use a supported web browser.

When you access the QRadar system, you are prompted for a user name and a password. The user name and password must be configured in advance by the administrator.

The following table lists the supported versions of web browsers.

Table 4. Supported web browsers for QRadar products

Web browser	Supported versions
Mozilla Firefox	38.0 Extended Support Release
32-bit Microsoft Internet Explorer, with document mode and browser mode enabled	10.0 11.0
Google Chrome	Version 46

Upgrade priority order in distributed deployments

When you upgrade IBM Security QRadar systems, you must complete the upgrade process on your Console first. You must be able to access the user interface on your desktop system before you upgrade your secondary Console and managed hosts.

Upgrade your QRadar systems in the following order:

1. Console
2. The following QRadar systems can be upgrade concurrently:
   - Event Processors
   - QRadar Event Collectors
   - Flow Processors
   - QFlow Collectors

Upgrades in HA deployments

If you upgrade IBM Security QRadar in high-availability (HA) deployments, the primary host must be the active system in your deployment. If the primary system is the active system and the secondary system is in standby mode, the upgrade is automatically applied to the associated secondary system.

If the HA cluster is disconnected, or you want to add a new secondary HA host, you must reinstall QRadar on the secondary HA. For more information about reinstalling software, see the *Installation Guide* for your system. After you reinstall the secondary HA host, log in to the user interface to reconnect or to create a new HA cluster.

Important: Disk replication and failover are disabled until the primary and secondary hosts synchronize and the `needs upgrade` or `failed` status is cleared from the secondary host.

After you upgrade the secondary host, you might be required to restore the configuration of the secondary host. For more information about restoring a failed host, see the *Administration Guide* for your product.

Chapter 2. Upgrading QRadar products

You must upgrade all of your IBM Security QRadar products in your deployment to the same version. During the upgrade, the version of RedHat Enterprise Linux is upgraded to version 6.7.

Before you begin

Ensure that you take the following precautions:

- Back up your data.

  For more information about backup and recovery, see the *Administration Guide* for your product.
- To avoid access errors in your log file, close all open QRadar product sessions.
- Ensure that you have sufficient RAM.

  During the upgrade from versions 7.1.x to 7.2.x, a system pretest checks that the minimum amount of RAM is available. If there is not enough RAM, the upgrade stops.
- If your deployment includes offboard storage solutions, you must disconnect your offboard storage.

  After you complete the upgrade, you can remount your external storage solutions. For more information, see the *Offboard Storage Guide*.

Procedure

1. Download the <*QRadar_patchupdate*>.*sfs* file from Fix Central (www.ibm.com/support/fixcentral).
2. Use SSH to log in to your system as the root user.
3. Copy the patch file to the `/tmp` directory or to another location that has sufficient disk space.
4. To create the `/media/updates` directory, type the following command:

   ```
   mkdir -p /media/updates
   ```
5. Change to the directory where you copied the patch file.
6. To mount the patch file to the `/media/updates` directory, type the following command:

   ```
   mount -o loop -t squashfs <QRadar_patchupdate>.sfs /media/updates/
   ```
7. To run the patch installer, type the following command:

   ```
   /media/updates/installer
   ```

   The first time that you run the patch installer script, there might be a delay before the first patch installer menu is displayed.
8. Provide answers to the pre-patch questions based on your QRadar deployment.
9. Using the patch installer, upgrade all systems in your deployment.

   If you do not select **Patch All**, you must upgrade systems in the following order:

   - Console
   - Event Processors
   - Event Collectors
   - Flow Processors

If your SSH session is disconnected while the upgrade is in progress, the upgrade continues. When you reopen your SSH session and rerun the installer, the installation resumes.

10. After the upgrade is complete, unmount the software update by using the following command: **umount /media/updates**

What to do next

1. Perform an automatic update to ensure that your configuration files contain the latest network security information. For more information, see the *IBM Security QRadar SIEM Administration Guide*.
2. Clear your Java™ cache and your web browser cache. After you upgrade QRadar, the **Vulnerabilities** tab might not be displayed. To use QRadar Vulnerability Manager after you upgrade, you must upload and allocate a valid license key. For more information, see the *Administration Guide* for your product.

Clearing the Java cache and web browser cache after upgrades

After you upgrade, clear the Java cache and web browser cache before you log in to IBM Security QRadar.

Before you begin

The Java Runtime Environment version 1.7 must be installed on the desktop system that you use to view the user interface.

Procedure

1. To clear the Java cache, open the Windows **Control Panel** search and enter `Java Control Panel`.
   a. View the **Temporary Internet Files**.
   b. Delete all of the QRadar Deployment Editor entries.
2. To clear you web browser cache, ensure that you have only one instance of your web browser open, and then clear the cache.
3. Log in to QRadar by typing the IP address of the QRadar system into a web browser:

   `https://`*`IP Address`*

   The default user name is `admin`.

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® 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 www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM

Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Index

Printed in USA