

IBM Security QRadar
Version 7 Release 3

Community Edition

IBM

Note

Before you use this information and the product that it supports, read the information in “Notices” on page 7.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.3.0 and subsequent releases unless superseded by an updated version of this document.

© Copyright IBM Corporation 2017, 2017.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

QRadar Community Edition Overview	1
Installing QRadar Community Edition.	2
Getting events from sources that are not supported by the default installation	3
Getting Started with QRadar Community Edition	4
Notices	7
Trademarks.	8
Terms and conditions for product documentation	9
IBM Online Privacy Statement	10

QRadar Community Edition Overview

QRadar® Community Edition is a free version of IBM® Security QRadar intended for individual use.

IBM QRadar Community Edition provides many of the same capabilities as QRadar with a license for 50 events per second and 5,000 flows per minute.

Anyone can download and try QRadar Community Edition for free. Download Community Edition if:

- You are a SOC analyst who wants to try QRadar in your environment to see whether the integrated analytic platform is a good fit for your organization.
- You are a developer who is creating QRadar apps, and you need an environment where you can test apps without affecting your production QRadar system.
- You are a QRadar user who needs to test and validate new use cases without affecting your production QRadar system.

The following table shows the features that are supported in QRadar Community Edition:

Table 1. Comparison of QRadar capabilities

Capability	QRadar SIEM	QRadar Community Edition
Full administrative capabilities	Yes	Yes
Customizable dashboards	Yes	Yes
Custom rules engine	Yes	Yes
Manage network and security events	Yes	Yes
Manage host and application logs	Yes	Yes
Threshold-based alerts	Yes	Yes
Compliance templates	Yes	Yes
Data archiving	Yes	Yes
WinCollect stand-alone deployments*	Yes	Yes
WinCollect managed deployments*	Yes	Yes
Network activity monitoring	Yes	Yes
Asset profiling	Yes	Yes
Offenses management	Yes	Yes
Network flow capture and analysis	Yes	Yes
Auto-updates	Yes	Yes
IBM Security X-Force® Threat Intelligence IP reputation feed integration	Yes	No
Historical correlation	Yes	No
Offline forwarding	Yes	No
QRadar Vulnerability Manager	Yes	No

Table 1. Comparison of QRadar capabilities (continued)

Capability	QRadar SIEM	QRadar Community Edition
QRadar Risk Manager integration	Yes	No
QRadar Incident Forensics integration	Yes	No
QRadar Network Insights integration	Yes	No
High Availability	Yes	No
Uploading a license	Yes	No
Software upgrades	Yes	No

* You need an IBM customer number to access WinCollect from IBM Fix Central.

Installing QRadar Community Edition

Install IBM Security QRadar Community Edition in a virtual machine. Community Edition is based on QRadar 7.3.0, and is released without a warranty.

Before you begin

You must have a system with a CentOS Linux 7.3 minimal installation that is connected to the internet, and that meets the following requirements to install QRadar Community Edition. Use 8 GB for the SWAP partition and the defaults for other partitions when you install your operating system. Disable SELinux to avoid a system restart during installation.

Note: QRadar Community Edition can't be installed in a Docker container.

Table 2. System requirements for QRadar Community Edition

Requirement	Description
Memory (RAM)	Minimum: 4 GB Note: You might need more RAM (or an app node) for some apps.
Free disk space	Minimum: 80 GB Optimal: 130 GB or higher
Processor	Minimum 2 CPU cores
Network adapter	You need at least one network adapter. Note: If you are using a locally hosted virtual machine with a local IP address, you must forward port 8444 to port 443 to access QRadar in a web browser, and forward port 2222 to port 22 to use ssh to connect to QRadar.

Procedure

1. Download the QRadar Community Edition ISO from IBM developerWorks® (<https://developer.ibm.com/qradar/>).
2. Copy the ISO to /tmp.
3. Create a /media/cdrom directory by using the following command:
`sudo mkdir /media/cdrom`
4. Mount the QRadar Community Edition ISO by using the following command:

```
sudo mount -o loop /tmp/<qradar_community_edition.iso> /media/cdrom
```

5. Run the QRadar setup by using the following command:

```
sudo /media/cdrom/setup
```

Note: If you didn't disable SELinux before installation, your QRadar Community Edition system restarts during the setup. After the system restarts, repeat steps 4 and 5.

6. Follow the instructions in the installation wizard.

Note: Passwords must contain at least 3 of the following attributes:

- uppercase characters
- lowercase characters
- special characters
- numbers

Results

You can access QRadar Community Edition in a web browser at https://<ip_address>/console. If you are using a locally hosted virtual machine with a local IP address, you can access QRadar Community Edition in a web browser on your host system at https://<ip_address>:8444/console.

What to do next

See “Getting Started with QRadar Community Edition” on page 4.

Getting events from sources that are not supported by the default installation

To monitor events from software, devices, or appliances that aren't supported by the default installation of IBM QRadar Community Edition, you must install a DSM (Device Support Module).

About this task

A *Device Support Module (DSM)* is a file that parses received events from multiple log sources and converts them to a format that QRadar understands. Each type of log source has a corresponding DSM.

The *IBM Security QRadar DSM Configuration Guide* lists the DSMs that are supported in QRadar. Only a few of the available DSMs are included by default in QRadar Community Edition, but you can add others.

The following DSMs are included by default in QRadar Community Edition:

- DSM-AssetProfiler
- DSM-SymantecEndpointProtection
- DSM-BluecoatProxySG
- DSM-IBMCustomerDSM
- DSM-IBMHealthMetrics
- DSM-IBMSense
- DSM-GNULinuxServer
- DSM-OracleDbAudit

- DSM-PaloAltoPaSeries
- DSM-SourceFireSnort
- DSM-SIMNotification
- DSM-SIMAudit
- DSM-SearchResults
- DSM-STEALTHbitsStealthINTERCEPT
- DSM-IBMHealthMetrics
- DSM-SIMGenericLog
- DSM-UniversalCEF
- DSM-UniversalLEEF
- DSM-SIMUniversal
- DSM-McAfeeIntrushield
- PROTOCOL-IBMSIMJDBC
- PROTOCOL-JDBC
- PROTOCOL-LEA
- PROTOCOL-LogFileProtocol
- PROTOCOL-JdbcSophos
- PROTOCOL-TCPSyslog

Procedure

1. To mount the ISO for QRadar Community Edition type the following command:

```
sudo mount -o loop /tmp/<qradar_community_edition.iso> /media/cdrom
```
2. Go to the /media/cdrom/post/dsmrpms directory by using the following command:

```
cd /media/cdrom/post/dsmrpms
```
3. Type the following command, where *<rpm_filename>* is the name of a DSM that you want to install:

```
yum -y install <rpm_filename>
```
4. Log in to the QRadar Community Edition user interface.
5. On the **Admin** tab, click **Deploy Changes**.
6. On the **Admin** tab, select **Advanced** > **Restart Web Services**.

What to do next

See the *IBM Security QRadar DSM Configuration Guide* to help you add a log source.

Getting Started with QRadar Community Edition

Depending on who you are, there are next steps to take:

- If you're a SOC analyst, you need to feed data into QRadar Community Edition. See "Getting events from sources that are not supported by the default installation" on page 3.
- If you're a developer, you need to understand the QRadar app framework.
 - See QRadar App Development on IBM developerWorks (<https://developer.ibm.com/qradar/>) to download the QRadar SDK.

- Check out information about QRadar apps (https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.appfw.doc/c_appframework_Extintro.html).
- If you're a user, you need to get an overview of how QRadar works.
 - Check out the Getting Started topics in the Knowledge Center (https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_oview.html).
 - Watch some QRadar videos, and see other training material in the IBM Security Learning Academy (<https://www.securitylearningacademy.com/local/navigator/index.php?level=sisi01>).

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

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

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.

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 actual people or business enterprises is entirely coincidental.

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 www.ibm.com/legal/copytrade.shtml.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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



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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING

BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

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>.



Printed in USA