IBM Security QRadar
Version 7.3.1

# *Community Edition*

**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This document applies to IBM QRadar Security Intelligence Platform V7.3.1 and subsequent releases unless superseded by an updated version of this document.

# Contents

# QRadar Community Edition Overview

IBM QRadar® Community Edition is a free version of IBM® Security QRadar intended for individual use, and is released without a warranty.

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 | Yes |
| Historical correlation | Yes | No |
| Offline forwarding | Yes | No |
| QRadar Vulnerability Manager | Yes | No |
| QRadar Risk Manager integration | Yes | No |
| QRadar Incident Forensics integration | Yes | No |
| QRadar Network Insights integration | Yes | No |

*Table 1. Comparison of QRadar capabilities (continued)*

| Capability | QRadar SIEM | QRadar Community Edition |
|---|---|---|
| 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.

For help with QRadar Community Edition, visit the developerWorks forum (https://developer.ibm.com/answers/topics/qradarce/?sort=newest&filter=all).

## System requirements for QRadar Community Edition

You must have a system with a CentOS Linux or RHEL 7.5 minimal installation that meets the following requirements to install QRadar Community Edition.

*Table 2. System requirements for QRadar Community Edition*

| Requirement | Description |
|---|---|
| Memory (RAM) | Minimum: 6 GB<br>**Note:** You need 8 GB if you are using X-Force tests or Ariel queries. You might need more RAM (or an app node) for some apps. |
| Free disk space | Minimum: 110 GB<br>Optimal: 130 GB or higher |
| Processor | Minimum 2 CPU cores<br>**Note:** For optimal performance, you need a minimum of 6 CPU cores if you are using X-force tests. You need a minimum of 8 CPU cores if you are using Ariel queries with X-force data. |
| Network adapter | You need at least one network adapter with access to the internet.<br>**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. Forward port 2222 to port 22 to use ssh to connect to QRadar. |

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

## Installing an operating system for QRadar Community Edition

You must install a CentOS Linux or RHEL V7.5 minimal operating system for QRadar Community Edition.

### About this task

- Your system must meet the requirements that are listed in “System requirements for QRadar Community Edition.”
- Your system must have internet access, or QRadar Community Edition installation fails.
- Use 8 GB for the SWAP partition and the defaults for other partitions.
- Disable SELinux. Restart your system after you disable SELinux or the installation fails.
- QRadar Community Edition can't be installed in a Docker container.

See the RHEL documentation (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/) for help installing and configuring CentOS or RHEL.

## Procedure

1. Select the USB or DVD drive as the boot option.
2. When prompted, log in to the system as the root user.
3. Follow the instructions in the installation wizard to complete the installation:
   a. Set the language to English (US).
   b. Click **Date & Time** and set the time for your deployment.
   c. Click **Installation Destination** and select the **I will configure partitioning** option.
   d. Click **Click here to create them automatically** to create the default mount points.
   e. Set the `/swap` partition to a minimum of 8 GB if it isn't already, and then click **Done**.
   f. Click **Accept Changes**.
   g. Click **Network & Host Name**.
   h. Enter the host name for your appliance.
   i. Select the interface in the list, move the switch to the **ON** position, and click **Configure**.
   j. On the **General** tab, select the **Automatically connect to this network when it is available** option.
   k. On the **IPv4 Settings** tab, select **Manual** in the **Method** list.
   l. Click **Add** to enter the IP address, Netmask, and Gateway for the appliance in the **Addresses** field.
   m. Add two DNS servers.
   n. Click **Save** > **Done** > **Begin Installation**.
4. Set the root password, and then click **Finish configuration**.
5. Disable SELinux and restart the appliance after the installation finishes.

## What to do next

"Installing QRadar Community Edition"

# Installing QRadar Community Edition

Install IBM Security QRadar Community Edition on CentOS or Red Hat Enterprise Linux (RHEL) in a virtual machine. Community Edition is based on QRadar 7.3.1.

## Before you begin

You must have a system with a CentOS Linux or RHEL 7.5 minimal installation that meets the following requirements to install QRadar Community Edition. See "Installing an operating system for QRadar Community Edition" on page 2.

**Notes:**

- QRadar Community Edition can't be installed in a Docker container.
- It is not possible to uninstall QRadar Community Edition, or to restart the installation process if it fails after the initial prechecks. Consider creating a snapshot of your operating system before you begin.

## Procedure

1. Verify that you have internet access on the appliance.
2. Download the QRadar Community Edition ISO from IBM developerWorks® (https://developer.ibm.com/qradar/ce/).
3. Copy the ISO to `/tmp`.
4. Create a `/media/cdrom` directory by using the following command:
   ```
   sudo mkdir /media/cdrom
   ```
5. Mount the QRadar Community Edition ISO by using the following command:

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

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

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

7. When prompted, restart your system to apply a kernel update. After you restart the system, repeat steps 4 and 5.
8. Set the admin password by typing the following command:

   ```
   sudo /opt/qradar/support/changePasswd.sh -a
   ```

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

   - Uppercase characters
   - Lowercase characters
   - Special characters
   - Numbers

9. Restart tomcat by typing the following command:

   ```
   sudo systemctl restart tomcat
   ```

10. Log in to QRadar Community Edition user interface and accept the EULA. 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.”

## 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.”
- 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_7.3.1/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_7.3.1/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).

## 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 code module that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as output. Each type of log source has a corresponding DSM.

The *IBM Security QRadar DSM Configuration Guide* (http://public.dhe.ibm.com/software/security/products/qradar/documents/iTeam_addendum/b_dsm_guide.pdf) 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-BluecoatProxySG
- DSM-IBMCustomDSM
- DSM-IBMHealthMetrics
- DSM-IBMSense
- DSM-GNULinuxServer
- DSM-McAfeeIntrushield
- DSM-MicrosoftWindows
- DSM-OracleDbAudit
- DSM-PaloAltoPaSeries
- DSM-SearchResults
- DSM-SIMNotification
- DSM-SIMAudit
- DSM-SIMGenericLog
- DSM-SIMUniversal
- DSM-SourceFireSnort
- DSM-STEALTHbitsStealthINTERCEPT
- DSM-SymantecEndpointProtection
- DSM-UniversalCEF
- DSM-UniversalLEEF
- PROTOCOL-IBMSIMJDBC
- PROTOCOL-JDBC
- PROTOCOL-JdbcSophos
- PROTOCOL-LEA
- PROTOCOL-LogFileProtocol
- PROTOCOL-TCPSyslog

## Procedure

1. Mount the QRadar Community Edition ISO by using 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 Server**.

## What to do next

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

# 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® 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.

Java™
COMPATIBLE

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.

## General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: https://ibm.com/gdpr

Printed in USA