

IBM QRadar  
Version 7.3.3

*Installation Guide*



**Note**

Before you use this information and the product that it supports, read the information in [“Notices” on page 65](#).

**Product information**

This document applies to IBM® QRadar® Security Intelligence Platform V7.3.3 and subsequent releases unless superseded by an updated version of this document.

© **Copyright International Business Machines Corporation 2004, 2019.**

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

---

# Contents

<b>Introduction to QRadar installations .....</b>	<b>V</b>
<b>Chapter 1. QRadar deployment overview.....</b>	<b>1</b>
License keys.....	1
Integrated Management Module.....	1
Prerequisite hardware accessories for QRadar installations.....	2
Environmental restrictions.....	2
Supported web browsers .....	2
Firmware update.....	3
Bandwidth for managed hosts.....	3
USB flash drive installations.....	3
Creating a bootable USB flash drive with Microsoft Windows.....	4
Creating a bootable USB flash drive on a Apple Mac OS X system.....	4
Creating a bootable USB flash drive with Red Hat Linux.....	5
Installing QRadar with a USB flash drive.....	6
Standard Linux users .....	6
Third-party software on QRadar appliances.....	8
<b>Chapter 2. QRadar installations.....</b>	<b>9</b>
Installing a QRadar appliance.....	9
QRadar software installations.....	10
Prerequisites for installing QRadar on your hardware.....	11
Installing RHEL on your hardware.....	12
Installing QRadar after the RHEL installation.....	14
<b>Chapter 3. Virtual appliance installations.....</b>	<b>17</b>
Overview of supported virtual appliances .....	17
System requirements for virtual appliances.....	20
Creating your virtual machine.....	24
Installing QRadar on a virtual machine.....	25
Adding your virtual appliance to your deployment.....	26
<b>Chapter 4. Installations from the recovery partition.....</b>	<b>27</b>
Reinstalling from the recovery partition.....	27
<b>Chapter 5. Reinstalling QRadar from media.....</b>	<b>29</b>
<b>Chapter 6. Setting up a QRadar silent installation.....</b>	<b>31</b>
<b>Chapter 7. Overview of QRadar deployment in a cloud environment.....</b>	<b>37</b>
Configuring a QRadar host on Amazon Web Services.....	37
Configuring server endpoints for cloud installations.....	39
Configuring client networks for cloud installations.....	40
Configuring a member for cloud installations.....	42
<b>Chapter 8. Configuring bonded management interfaces.....</b>	<b>43</b>
<b>Chapter 9. Network settings management.....</b>	<b>45</b>
Changing the network settings in an all-in-one system.....	45

Changing the network settings of a QRadar Console in a multi-system deployment.....	46
Updating network settings after a NIC replacement.....	47
<b>Chapter 10. Troubleshooting problems.....</b>	<b>49</b>
Troubleshooting resources.....	49
Support Portal.....	50
Service requests .....	50
Fix Central.....	50
Knowledge bases.....	51
QRadar log files.....	51
Common ports and servers used by QRadar.....	52
QRadar port usage .....	52
Viewing IMQ port associations.....	59
Searching for ports in use by QRadar.....	60
QRadar public servers.....	60
<b>Chapter 11. Receiving QRadar update notifications.....</b>	<b>63</b>
<b>Notices.....</b>	<b>65</b>
Trademarks.....	66
Terms and conditions for product documentation.....	66
IBM Online Privacy Statement.....	67
General Data Protection Regulation.....	67

# Introduction to QRadar installations

---

IBM QRadar appliances are pre-installed with software and the Red Hat Enterprise Linux® operating system. You can also install QRadar software on your own hardware.

Thank you for ordering your appliance from IBM! It is strongly recommended that you apply the latest maintenance to your appliance for the best results. Please visit IBM Fix Central (<http://www.ibm.com/support/fixcentral>) to determine the latest recommended patch for your product.

To install or recover a high-availability (HA) system, see the *IBM QRadar High Availability Guide*.

## Intended audience

Network administrators who are responsible for installing and configuring QRadar systems must be familiar with network security concepts and the Linux operating system.

## Technical documentation

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

For information about how to access more technical documentation in the QRadar products library, see [QRadar Support – Assistance 101](https://ibm.biz/qradarsupport) (<https://ibm.biz/qradarsupport>).

## Contacting customer support

For information about contacting customer support, see [QRadar Support – Assistance 101](https://ibm.biz/qradarsupport) (<https://ibm.biz/qradarsupport>).

## 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 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 QRadar.



---

# Chapter 1. QRadar deployment overview

You can install IBM QRadar on a single server for small enterprises, or across multiple servers for large enterprise environments.

For maximum performance and scalability, you must install a high-availability (HA) managed host appliance for each system that requires HA protection. For more information about installing or recovering an HA system, see the *IBM QRadar High Availability Guide*.

## License keys

---

After you install IBM QRadar, you must apply your license keys.

Your system includes a temporary license key that provides you with access to QRadar software for five weeks. After you install the software and before the default license key expires, you must add your purchased licenses.

The following table describes the restrictions for the default license key:

Table 1. Restrictions for the default license key for QRadar SIEM installations	
Usage	Limit
Events per second threshold <b>Important:</b> This restriction also applies to the default license key for IBM QRadar Log Manager.	5000
Flows per interval	200000

When you purchase a QRadar product, an email that contains your permanent license key is sent from IBM. These license keys extend the capabilities of your appliance type and define your system operating parameters. You must apply your license keys before your default license expires.

### Related tasks

[Installing a QRadar appliance](#)

[Installing RHEL on your hardware](#)

You can install the Red Hat Enterprise Linux (RHEL) operating system on your hardware to use with IBM QRadar.

[Installing QRadar on a virtual machine](#)

After you create your virtual machine, you must install the IBM QRadar software on the virtual machine.

## Integrated Management Module

---

Use Integrated Management Module, which is on the back panel of each appliance type, for remote management of the hardware and operating systems, independent of the status of the managed server.

You can configure Integrated Management Module to share an Ethernet port with the IBM QRadar product management interface. However, to reduce the risk of losing the connection when the appliance is restarted, configure Integrated Management Module in dedicated mode.

To configure Integrated Management Module, you must access the system BIOS settings by pressing F1 when the IBM splash screen is displayed. For more information about configuring Integrated Management Module, see the *Integrated Management Module User's Guide* on the CD that is shipped with your appliance.

## Related concepts

[Prerequisite hardware accessories for QRadar installations](#)

Before you install IBM QRadar products, ensure that you have access to the required hardware accessories and desktop software.

## Prerequisite hardware accessories for QRadar installations

---

Before you install IBM QRadar products, ensure that you have access to the required hardware accessories and desktop software.

### Hardware accessories

Ensure that you have access to the following hardware components:

- Monitor and keyboard, or a serial console
- Uninterrupted Power Supply (UPS) for all systems that store data, such as QRadar Console, Event Processor components, or QRadar QFlow Collector components
- Null modem cable if you want to connect the system to a serial console

**Important:** QRadar products support hardware-based Redundant Array of Independent Disks (RAID) implementations, but do not support software-based RAID installations.

### Related tasks

[Installing a QRadar appliance](#)

[Installing RHEL on your hardware](#)

You can install the Red Hat Enterprise Linux (RHEL) operating system on your hardware to use with IBM QRadar.

[Installing QRadar on a virtual machine](#)

After you create your virtual machine, you must install the IBM QRadar software on the virtual machine.

## Environmental restrictions

---

QRadar performance can be affected by other devices in your deployment.

For any DNS server that you point a QRadar appliance to, you cannot have a DNS registry entry with the hostname set to localhost.

## Supported web browsers

---

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

The following table lists the supported versions of web browsers.

Table 2. Supported web browsers for QRadar products	
Web browser	Supported versions
64-bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later
Microsoft Internet Explorer	11.0
64-bit Google Chrome	Latest



## Security exceptions and certificates

If you are using the Mozilla Firefox web browser, you must add an exception to Mozilla Firefox to log in to QRadar SIEM. For more information, see your Mozilla Firefox web browser documentation.

If you are using the Microsoft Internet Explorer web browser, a website security certificate message is displayed when you access the QRadar SIEM system. You must select the **Continue to this website option** to log in to QRadar SIEM.

## Navigate the web-based application

When you use QRadar SIEM, use the navigation options available in the QRadar SIEM user interface instead of your web browser **Back** button.

## Firmware update

---

Update the firmware on IBM QRadar appliances to take advantage of additional features and updates for the internal hardware components.

For more information about updating firmware, see [Firmware update for QRadar \(http://www-01.ibm.com/support/docview.wss?uid=swg27047121\)](http://www-01.ibm.com/support/docview.wss?uid=swg27047121).

## Bandwidth for managed hosts

---

To replicate state and configuration data, ensure that you have a minimum bandwidth of 100 Mbps between the IBM QRadar console and all managed hosts. Higher bandwidth is necessary when you search log and network activity, and you have over 10,000 events per second (EPS).

An Event Collector that is configured to store and forward data to an Event Processor forwards the data according to the schedule that you set. Ensure that you have sufficient bandwidth to cover the amount of data that is collected, otherwise the forwarding appliance cannot maintain the scheduled pace.

Use the following methods to mitigate bandwidth limitations between data centers:

### Process and send data to hosts at the primary data center

Design your deployment to process and send data as it's collected to hosts at the primary data center where the console resides. In this design, all user-based searches query the data from the local data center rather than waiting for remote sites to send back data.

You can deploy a store and forward event collector, such as a QRadar 15XX physical or virtual appliance, in the remote locations to control bursts of data across the network. Bandwidth is used in the remote locations, and searches for data occur at the primary data center, rather than at a remote location.

### Don't run data-intensive searches over limited bandwidth connections

Ensure that users don't run data-intensive searches over links that have limited bandwidth. Specifying precise filters on the search limits the amount of data that is retrieved from the remote locations, and reduces the bandwidth that is required to send the query result back.

For more information about deploying managed hosts and components after installation, see the *IBM QRadar Administration Guide*.

## USB flash drive installations

---

You can install IBM QRadar software with a USB flash drive.

USB flash drive installations are full product installations. You cannot use a USB flash drive to upgrade or apply product patches. For information about applying fix packs, see the fix pack Release Notes.

## Supported versions

The following appliances or operating systems can be used to create a bootable USB flash drive:

- A Linux system that is installed with Red Hat Enterprise Linux V7.5
- Apple Mac OS X
- Microsoft Windows

## Installation overview

Follow this procedure to install QRadar software from a USB flash drive:

1. Create the bootable USB flash drive.
2. Install the software for your QRadar appliance.
3. Install any product maintenance releases or fix packs.

See the Release Notes for installation instructions for fix packs and maintenance releases.

## Creating a bootable USB flash drive with Microsoft Windows

You can use a Microsoft Windows desktop or notebook system to create a bootable USB flash drive that you can use to install QRadar software.

### Before you begin

You must have access to the following items:

- An 8 GB or larger USB flash drive
- A desktop or notebook system running Microsoft Windows

### Procedure

1. Download the QRadar ISO image file from [Fix Central](http://www.ibm.com/support/fixcentral/) ([www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/)).
2. Follow the instructions in the Red Hat Enterprise Linux documentation for [making installation USB media on Windows](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/installation_guide/sect-making-usb-media#sect-making-usb-media-windows) ([https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/installation\\_guide/sect-making-usb-media#sect-making-usb-media-windows](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/installation_guide/sect-making-usb-media#sect-making-usb-media-windows)).

### What to do next

See [Installing QRadar with a USB flash drive](#).

## Creating a bootable USB flash drive on a Apple Mac OS X system

You can use an Apple Mac OS X computer to create a bootable USB flash drive that you can use to install QRadar software.

### Before you begin

You must have access to the following items:

- An 8 GB or larger USB flash drive
- A QRadar V7.3.1 or later ISO image file

### About this task

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

### Procedure

1. Download the QRadar ISO image file from [Fix Central](http://www.ibm.com/support/fixcentral/) ([www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/)).
2. Insert the USB flash drive into a USB port on your system.

3. Open a terminal and type the following command to unmount the USB flash drive:

```
diskutil unmountDisk /dev/<name_of_the_connected_USB_flash_drive>
```

4. Type the following command to write the QRadar ISO to your USB flash drive:

```
dd if=<qradar>.iso of=/dev/r<name_of_the_connected_USB_flash_drive> bs=1m
```

**Note:** The "r" before the name of the connected USB flash drive is for raw mode, which makes the transfer much faster. There is no space between the "r" and the name of the connected USB flash drive.

5. Remove the USB flash drive from your system.

### What to do next

See [Installing QRadar with a USB flash drive](#).

## Creating a bootable USB flash drive with Red Hat Linux

You can use a desktop or notebook system with Red Hat Enterprise Linux V7.5 to create a bootable USB flash drive that you can use to install QRadar software.

### Before you begin

You must have access to the following items:

- An 8 GB or larger USB flash drive
- A QRadar V7.3.1 or later ISO image file

### About this task

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

### Procedure

1. Download the QRadar ISO image file from [Fix Central](http://www.ibm.com/support/fixcentral/) (www.ibm.com/support/fixcentral/).
2. Insert the USB flash drive into a USB port on your system.  
  
It might take up to 30 seconds for the system to recognize the USB flash drive.
3. Open a terminal and type the following command to determine the name of the USB flash drive:

```
dmesg | grep SCSI
```

The system outputs the messages produced by device drivers. The following example shows the name of the connected USB flash drive as *sdb*.

```
[ 170.171135] sd 5:0:0:0: [sdb] Attached SCSI removable disk
```

4. Type the following commands to unmount the USB flash drive:

```
df -h | grep <name_of_the_connected_USB_flash_drive>  
umount /dev/<name_of_the_connected_USB_flash_drive>
```

5. Type the following command to write the QRadar ISO to your USB flash drive:

```
dd if=<qradar>.iso of=/dev/<name_of_the_connected_USB_flash_drive> bs=512k
```

6. Remove the USB flash drive from your system.

### What to do next

See [Installing QRadar with a USB flash drive](#).

## Installing QRadar with a USB flash drive

Follow this procedure to install QRadar from a bootable USB flash drive.

### Before you begin

You must create the bootable USB flash drive before you can use it to install QRadar software.

### About this task

This procedure provides general guidance on how to use a bootable USB flash drive to install QRadar software.

The complete installation process is documented in the product Installation Guide.

### Procedure

1. Install all necessary hardware.
2. Choose one of the following options:
  - Connect a notebook to the serial port at the back of the appliance.
  - Connect a keyboard and monitor to their respective ports.
3. Insert the bootable USB flash drive into the USB port of your appliance.
4. Restart the appliance.

Most appliances can boot from a USB flash drive by default. If you are installing QRadar software on your own hardware, you might have to set the device boot order to prioritize USB.

After the appliance starts, the USB flash drive prepares the appliance for installation. This process can take up to an hour to complete.

5. When the **Red Hat Enterprise Linux** menu is displayed, select one of the following options:
  - If you connected a keyboard and monitor, select **Install Red Hat Enterprise Linux 7.5**.
  - If you connected a notebook with a serial connection, select **Install Red Hat Enterprise Linux 7.5 using Serial console without format prompt** or **Install Red Hat Enterprise Linux 7.5 using Serial console with format prompt**.
6. Type **SETUP** to begin the installation.
7. When the login prompt is displayed, type **root** to log in to the system as the root user.

The user name is case-sensitive.
8. Press **Enter** and follow the prompts to install QRadar.

The complete installation process is documented in the product Installation Guide.

## Standard Linux users

The tables describe the standard Linux user accounts that are created on the QRadar console SIEM server and other QRadar product components (All In One console, QRadar Risk Manager, QRadar Incident Forensics, QRadar Network Insights, App Host, and all other managed hosts).

The following tables show standard Linux user accounts for RedHat and QRadar.

Table 3. Standard Linux user accounts for RedHat		
User account	Login to the Login Shell	Purpose
root (password required)	Yes	RedHat user
bin	No	Linux Standard Base
daemon	No	Linux Standard Base

<i>Table 3. Standard Linux user accounts for RedHat (continued)</i>		
<b>User account</b>	<b>Login to the Login Shell</b>	<b>Purpose</b>
adm	No	Linux Standard Base
lp	No	Linux Standard Base
sync	No	Linux Standard Base
shutdown	No	Linux Standard Base
halt	No	Linux Standard Base
mail	No	Linux Standard Base
operator	No	Linux Standard Base
games	No	RedHat user
ftp	No	RedHat user
nobody	No	Linux Standard Base
systemd-network	No	RedHat user
dbus	No	RedHat user
polkitd	No	RedHat user
sshd	No	RedHat user
rpc	No	RedHat user
rpcuser	No	RedHat user
nfsnobody	No	RedHat user
abrt	No	RedHat user
ntp	No	RedHat user
tcpdump	No	RedHat user
tss	No	RedHat user
saslauth	No	RedHat user
sssd	No	RedHat user

<i>Table 4. Standard Linux user accounts for QRadar</i>		
<b>User Account</b>	<b>Login to the Login Shell</b>	<b>Purpose</b>
ziptie	No	Ziptie service used by QRadar Risk Manager
si-vault	No	QRadar Vault service used by QRadar to store secrets and manage internal certificates
vis	No	QRadar VIS service used by QRadar to process scan results
si-registry	No	QRadar Docker Registry Service used by QRadar for App Framework
customactionuser	No	QRadar Custom Actions used to isolate custom actions into a chroot jail
mks	No	MKS QRadar component for handling secrets

<i>Table 4. Standard Linux user accounts for QRadar (continued)</i>		
<b>User Account</b>	<b>Login to the Login Shell</b>	<b>Purpose</b>
qradar	No	General user for QRadar
qvmuser	No	QRadar Vulnerability Manager used by QRadar Vulnerability Manager
postgres	No (account locked)	PostgreSQL database used by QRadar
tlsdated	No	Tlsdate legacy time sync tool that was previously used by QRadar
traefik	No	Traefik service proxies Docker Containers for QRadar App Framework
gluster	No	GlusterFS used by QRadar HA on event collectors
solr	No	Solr service used by QRadar Forensics
openvpn	No	OpenVPN optional VPN tool installed by QRadar
chrony	No	Chronyd service time sync tool used by QRadar
apache	No	Apache Web Server used by QRadar
postfix	No	Mail Service used by QRadar to send email

## Third-party software on QRadar appliances

IBM QRadar is a security appliance that is built on Linux, and is designed to resist attacks. QRadar is not intended as a multi-user, general-purpose server. It is designed and developed specifically to support its intended functions. The operating system and the services are designed for secure operation. QRadar has a built-in firewall, and allows administrative access only through a secure connection that requires encrypted and authenticated access, and provides controlled upgrades and updates. QRadar does not require or support traditional anti-virus or malware agents, or support the installation of third-party packages or programs.

---

## Chapter 2. QRadar installations

There are two ways to install QRadar on your hardware: a software installation, or an appliance installation.

### Appliance installation

An appliance installation is a QRadar installation that uses the version of Red Hat Enterprise Linux (RHEL) included in the QRadar ISO. An appliance installation on your own hardware or in a virtual machine requires you to purchase a software node entitlement. Contact your QRadar sales representative for more information about purchasing a software node entitlement. You do not need to configure partitions or perform other RHEL preparation as part of an appliance installation. Choose this option, if RHEL is not already installed. Proceed to [“Installing a QRadar appliance” on page 9](#). However, if the hardware/virtual instance configuration varies from our listed specifications, the version of RHEL included in the QRadar ISO may not install properly. In that case, you should attempt a software installation.

### Software installation

A software installation is a QRadar installation that uses a RHEL operating system that you provide. The RHEL version required for your installment must be provided by a 3rd party. You must configure partitions and perform other RHEL preparations before a QRadar software installation. Aside from RHEL, all software installations requires you to purchase a software node entitlement. Contact your QRadar sales representative for more information about purchasing a software node entitlement. Proceed to [“QRadar software installations” on page 10](#).

---

## Installing a QRadar appliance

Install a IBM QRadar Console or a managed host on a QRadar appliance or on your own appliance.

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

### Before you begin


Ensure that the following requirements are met:

- The required hardware is installed.
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection.
- If you want to configure bonded network interfaces, see [Chapter 8, “Configuring bonded management interfaces,” on page 43](#).
- If you are installing QRadar on a Unified Extensible Firmware Interface (UEFI) system, secure boot must be disabled.

### Procedure

1. Type `root` at the login prompt to launch the installation wizard. Type password if you are prompted for a password.
2. Accept the **End User License Agreement**.
3. Select the appliance type:
  - **Appliance Install**
  - **High Availability Appliance**
4. Select the appliance assignment, and then select **Next**.
5. If you selected an appliance for high-availability (HA), select whether the appliance is a console.
6. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.

7. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
8. Select the Internet Protocol version:
  - **ipv4**
  - **ipv6**If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.
  - manual**  
You must use a static IP address with a CIDR range.
  - auto**  
A static IP address with a CIDR range is generated with the Neighbor Discovery Protocol.
9. Select the bonded interface setup, if required.
10. Select the management interface.
11. In the wizard, enter a fully qualified domain name in the **Hostname** field.
12. In the **IP address** field, enter a static IP address, or use the assigned IP address.
13. If you do not have an email server, enter localhost in the **Email server name** field.
14. Enter a **root** password that meets the following criteria:
  - Contains at least 5 characters
  - Contains no spaces
  - Can include the following special characters: @, #, ^, and \*.
15. If you are installing a Console, enter an admin password that meets the same criteria as the **root** password.
16. Click **Finish**.
17. Follow the instructions in the installation wizard to complete the installation.

The installation process might take several minutes.
18. If you are installing a Console, apply your license key.
  - a) Log in to QRadar as the admin user:  
`https://<IP_Address_QRadar>`
  - b) Click **Login**.
  - c) On the navigation menu () , click **Admin**.
  - d) In the navigation pane, click **System Configuration**.
  - e) Click the **System and License Management** icon.
  - f) From the **Display** list box, select **Licenses**, and upload your license key.
  - g) Select the unallocated license and click **Allocate System to License**.
  - h) From the list of systems, select a system, and click **Allocate System to License**.
19. If you want to add managed hosts, see the *IBM QRadar Administration Guide*.

#### What to do next

Go to the (<https://apps.xforce.ibmcloud.com/>) to download *Security applications* for your installation. For more information, see the *Content Management* chapter in the *IBM QRadar Administration Guide*.

## QRadar software installations

---

A software installation is a QRadar installation on your hardware that uses an RHEL operating system that you provide. You must configure partitions and perform other RHEL preparation before a QRadar software installation.

#### Important:



- Ensure that your hardware meets the system requirements for QRadar deployments. For more information about system requirements, see [“Prerequisites for installing QRadar on your hardware” on page 11](#), [“System requirements for virtual appliances” on page 20](#), and [“Appliance storage requirements for virtual and software installations” on page 11](#).
- You must acquire entitlement to a QRadar Software Node for a QRadar software installation. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.
- Install no software other than QRadar and RHEL on your hardware. Unapproved RPM installations can cause dependency errors when you upgrade QRadar software and can also cause performance issues in your deployment.
- Do not update your operating system or packages before or after QRadar installation.
- If you are installing QRadar on a Unified Extensible Firmware Interface (UEFI) system, secure boot must be disabled.

Complete the following tasks in order:

- \_\_ • [“Installing RHEL on your hardware” on page 12](#)
- \_\_ • [“Installing QRadar after the RHEL installation” on page 14](#)

## Prerequisites for installing QRadar on your hardware

Before you install the Red Hat Enterprise Linux (RHEL) operating system on your hardware, ensure that your system meets the system requirements.

The following table describes the system requirements:

<i>Table 5. System requirements for RHEL installations on your own appliance</i>	
Requirement	Description
Supported OS	V7.5
Bit version	64-bit
KickStart disks	Not supported
Network Time Protocol (NTP) package	Optional If you want to use NTP as your time server, ensure that you install the NTP package.
Firewall configuration	WWW (http, https) enabled SSH-enabled
Hardware	See the tables below for memory, processor, and storage requirements.

### Appliance storage requirements for virtual and software installations

To install QRadar using virtual or software options the device must meet minimum storage requirements.

The following table shows the recommended minimum storage requirements for installing QRadar by using the virtual or software only option.

**Note:** The minimum required storage size will vary, based on factors such as event size, events per second (EPS), and retention requirements.

Table 6. Minimum storage requirements for appliances when you use the virtual or software installation option.

System classification	Appliance information	IOPS	Data transfer rate (MB/s)
Minimum performance	Supports XX05 licensing	800	500
Medium performance	Supports XX29 licensing	1200	1000
High Performance	Supports XX48 licensing	10,000	2000
Small All-in-One or 1600	Less than 500 EPS	300	300
Event/Flow Collectors	Events and flows	300	300

## Installing RHEL on your hardware

You can install the Red Hat Enterprise Linux (RHEL) operating system on your hardware to use with IBM QRadar.

### Before you begin

Download the Red Hat Enterprise Linux Server 7.5 x86\_64 Boot ISO from <https://access.redhat.com>.

### About this task

You must acquire entitlement to a QRadar Software Node for a QRadar software installation. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

If there are circumstances where you need to install RHEL separately, proceed with the following instructions. Otherwise, proceed to [“Installing a QRadar appliance” on page 9](#).

### Procedure

- Copy the RHEL ISO to a DVD or a bootable USB flash drive.
- Insert the portable storage device into your appliance and restart your appliance.
- From the starting menu, do one of the following options:
  - Select the USB or DVD drive as the boot option.
  - To install on a system that supports Extensible Firmware Interface (EFI), you must start the system in legacy mode.
- When prompted, log in to the system as the root user.
- Follow the instructions in the installation wizard to complete the installation:
  - Set the language to English (US).
  - Click **Date & Time** and set the time for your deployment.
  - Click **Software selection** and select **Minimal Install**.
  - Click **Installation Destination** and select the **I will configure partitioning** option.
  - Select **LVM** from the list.
  - Click the **Add** button to add the mount points and capacities for your partitions, and then click **Done**. For more information about RHEL7 partitions, see [“Linux operating system partition properties for QRadar installations on your own hardware” on page 13](#).
  - Click **Network & Host Name**.
  - Enter a fully qualified domain name for your appliance host name.
  - Select the interface in the list, move the switch to the **ON** position, and click **Configure**.
  - On the **General** tab, select the **Automatically connect to this network when it is available** option.
  - On the **IPv4 Settings** or **IPv6 Settings** tab, select **Manual** in the **Method** list.

- l) Click **Add**.
  - For an IPv4 deployment, enter the IP address, Netmask, and Gateway for the appliance in the **Addresses** field.
  - For an IPv6 deployment, enter the IP address, Prefix, and Gateway in the **Addresses** field.
- m) Add two DNS servers.
- n) Click **Save > Done > Begin Installation**.
6. Set the root password, and then click **Finish configuration**.
7. After the installation finishes, disable SELinux by modifying the `/etc/selinux/config` file, and restart the appliance.

### What to do next

[“Installing QRadar after the RHEL installation” on page 14](#)

### Linux operating system partition properties for QRadar installations on your own hardware

If you use your own appliance hardware, you can delete and re-create partitions on your Red Hat Enterprise Linux operating system rather than modify the default partitions.

Use the values in following table as a guide when you re-create the partitioning on your Red Hat Enterprise Linux operating system.

The file system for each partition is XFS.

Table 7. Partitioning guide for RHEL			
Mount Path	LVM supported?	Exists on Software Installation?	Size
/boot	No	Yes	1 GB
/boot/efi	No	Yes	200 MB
/recovery	No	No	8 GB
/var	Yes	Yes	5 GB
/var/log	Yes	Yes	15 GB
/var/log/audit	Yes	Yes	3 GB
/opt	Yes	Yes	10 GB
/home	Yes	Yes	1 GB
/storetmp	Yes	Yes	15 GB
/tmp	Yes	Yes	3 GB
swap	N/A	Yes	Swap formula: Configure the swap partition size to be 75 per cent of RAM, with a minimum value of 12 GiB and a maximum value of 24 GiB.
/	Yes	Yes	Up to 15 GB
/store	Yes	Yes	80% of remaining space
/transient	Yes	Yes	20% of remaining space

## Console partition configurations for multiple disk deployments

For hardware with multiple disks, configure the following partitions for QRadar:

### Disk 1

boot, swap, OS, QRadar temporary files, and log files

### Remaining disks

- Use the default storage configurations for QRadar appliances as a guideline to determine what RAID type to use.
- Mounted as /store
- Store QRadar data

The following table shows the default storage configuration for QRadar appliances.

Table 8. Default storage configurations for QRadar appliances	
QRadar host role	Storage configuration
Flow collector QRadar Network Insights (QNI)	RAID1
Data node Event processor Flow processor Event and flow processor All-in-one console	RAID6
Event collector	RAID10

## Installing QRadar after the RHEL installation

Install IBM QRadar on your own device after you install RHEL.

### Procedure

1. Copy the QRadar ISO to the /root or /storetmp directory of the device.
2. Create the /media/cdrom directory by typing the following command:

```
mkdir /media/cdrom
```

3. Mount the QRadar ISO by using the following command:

```
mount -o loop <path_to_ISO>/<qradar.iso> /media/cdrom
```

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

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

**Note:** A new kernel may be installed as part of the installation, which requires a system restart. Repeat the commands in steps 3 and 4 after the system restart to continue the installation.

5. Select the appliance type:
  - **Software Install**
  - **High Availability Appliance**
6. Select the appliance assignment, and then select **Next**.
7. If you selected an appliance for high-availability (HA), select whether the appliance is a console.


8. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.
9. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
10. Select the Internet Protocol version:
  - Select **ipv4** or **ipv6**.
11. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.
12. Select the bonded interface setup, if required.
13. Select the management interface.
14. In the wizard, enter a fully qualified domain name in the **Hostname** field.
15. In the **IP address** field, enter a static IP address, or use the assigned IP address.

**Important:** If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

For more information, see the *IBM Security QRadar High Availability Guide*.

16. If you do not have an email server, enter localhost in the **Email server name** field.
17. Leave the root password as it is.
18. If you are installing a Console, enter an admin password that meets the following criteria:
  - Contains at least 5 characters
  - Contains no spaces
  - Can include the following special characters: @, #, ^, and \*.
19. Click **Finish**.
20. Follow the instructions in the installation wizard to complete the installation.

The installation process might take several minutes.

21. If you are installing a Console, apply your license key.
  - a) Log in to QRadar as the admin user:  
`https://<IP_Address_QRadar>`
  - b) Click **Login**.
  - c) On the navigation menu () , click **Admin**.
  - d) In the navigation pane, click **System Configuration**.
  - e) Click the **System and License Management** icon.
  - f) From the **Display** list box, select **Licenses**, and upload your license key.
  - g) Select the unallocated license and click **Allocate System to License**.
  - h) From the list of systems, select a system, and click **Allocate System to License**.
22. If you want to add managed hosts, see the *IBM Security QRadar SIEM Administration Guide*.



---

## Chapter 3. Virtual appliance installations

You can install IBM QRadar SIEM on a virtual appliance. Ensure that you use a supported virtual appliance that meets the minimum system requirements.

There are two ways to install QRadar on your virtual appliance: a software installation, or an appliance installation.

### Appliance installation

An appliance installation is a QRadar installation that uses the version of Red Hat Enterprise Linux (RHEL) included in the QRadar ISO. An appliance installation on your own hardware or in a virtual machine requires you to purchase a software node entitlement. Contact your QRadar sales representative for more information about purchasing a software node entitlement. You do not need to configure partitions or perform other RHEL preparation as part of an appliance installation. Choose this option, if RHEL is not already installed. Proceed to Installing a QRadar appliance. However, if the hardware/virtual instance configuration varies from our listed specifications, the version of RHEL included in the QRadar ISO may not install properly. In that case, you should attempt a software installation.

### Software installation

A software installation is a QRadar installation that uses a RHEL operating system that you provide. The RHEL version required for your installment must be provided by a 3rd party. You must configure partitions and perform other RHEL preparations before a QRadar software installation. Aside from RHEL, all software installations requires you to purchase a software node entitlement. Contact your QRadar sales representative for more information about purchasing a software node entitlement. Proceed to QRadar software installations.

**Note:** If the installer does not detect that RHEL is installed, an appliance installation is performed automatically. You still see both the **Appliance Install (purchased as an appliance)** or **Software Install (hardware was purchased separately)** options in the installer menu. If RHEL is installed, only the **Software Install (hardware was purchased separately)** option appears.

To install a virtual appliance, complete the following tasks in order:

- Create a virtual machine.
- Install QRadar software on the virtual machine.
- If your virtual appliance is a managed host, add your virtual appliance to your deployment.

**Important:** Install no software other than QRadar and RHEL on your virtual machine.

---

## Overview of supported virtual appliances

A virtual appliance provides the same visibility and function in your virtual network infrastructure that QRadar appliances provide in your physical environment.

The following virtual appliances are available:

- QRadar SIEM All-in-One Virtual 3199
- QRadar SIEM Event and Flow Processor Virtual 1899
- QRadar SIEM Flow Processor Virtual 1799
- QRadar SIEM Event Processor Virtual 1699
- QRadar Event Collector Virtual 1599
- QRadar Data Node Virtual 1400
- QRadar QFlow Virtual 1299
- QRadar Risk Manager 700
- QRadar Vulnerability Manager Processor 600

- QRadar Vulnerability Manager Scanner 610
- QRadar App Host 4000
- QRadar Incident Forensics

### **QRadar SIEM All-in-One Virtual 3199**

This virtual appliance is a QRadar SIEM system that profiles network behavior and identifies network security threats. The QRadar SIEM All-in-One Virtual 3199 virtual appliance includes an onboard Event Collector, a combined Event Processor and Flow Processor, and internal storage for events.

The QRadar SIEM All-in-One Virtual 3199 virtual appliance supports the following items:

- Up to 1,000 network objects
- 1,200,000 flows per interval, depending on your license
- 30,000 Events Per Second (EPS), depending on your license
- External flow data sources for NetFlow, sFlow, J-Flow, Packeteer, and Flowlog files
- QRadar QFlow Collector and Layer 7 network activity monitoring

To expand the capacity of the QRadar SIEM All-in-One Virtual 3199 beyond the license-based upgrade options, you can add one or more of the QRadar SIEM Event Processor Virtual 1699 or QRadar SIEM Flow Processor Virtual 1799 virtual appliances.

### **QRadar SIEM Event and Flow Processor Virtual 1899**

This virtual appliance is deployed with any QRadar Console. The virtual appliance is used to increase storage and includes a combined Event Processor and Flow Processor and internal storage for events and flows.

QRadar SIEM Event and Flow Processor Virtual 1899 appliance supports the following items:

- 1,200,000 flows per interval, depending on traffic types
- 30,000 Events Per Second (EPS), depending on your license
- 2 TB or larger dedicated flow storage
- 1,000 network objects
- QRadar QFlow Collector and Layer 7 network activity monitoring

You can add QRadar SIEM Event and Flow Processor Virtual 1899 appliances to any QRadar Console to increase the storage and performance of your deployment.

### **QRadar SIEM Flow Processor Virtual 1799**

This virtual appliance is a dedicated Flow Processor that you can use to scale your QRadar SIEM deployment to manage higher flows per interval rates. The QRadar SIEM Flow Processor Virtual 1799 includes an onboard Flow Processor and internal storage for flows.

The QRadar SIEM Flow Processor Virtual 1799 appliance supports the following items:

- 3,600,000 flows per interval, depending on traffic types
- 2 TB or larger dedicated flow storage
- 1,000 network objects
- QRadar QFlow Collector and Layer 7 network activity monitoring

The QRadar SIEM Flow Processor Virtual 1799 appliance is a distributed Flow Processor appliance and requires a connection to any QRadar SIEM 31XX series appliance.



### **QRadar SIEM Event Processor Virtual 1699**

This virtual appliance is a dedicated Event Processor that you can use to scale your QRadar SIEM deployment to manage higher EPS rates. The QRadar SIEM Event Processor Virtual 1699 includes an onboard Event Collector, Event Processor, and internal storage for events.

The QRadar SIEM Event Processor Virtual 1699 appliance supports the following items:

- Up to 80,000 events per second
- 2 TB or larger dedicated event storage

The QRadar SIEM Event Processor Virtual 1699 virtual appliance is a distributed Event Processor appliance and requires a connection to any QRadar SIEM 31XX series appliance.

### **QRadar Event Collector Virtual 1599**

This virtual appliance is a dedicated Event Collector that you can use to scale your QRadar SIEM deployment to manage higher EPS rates. The QRadar Event Collector Virtual 1599 includes an onboard Event Collector.

The QRadar Event Collector Virtual 1599 appliance supports the following items:

- Up to 80,000 events per second
- 2 TB or larger dedicated event storage

The QRadar Event Collector Virtual 1599 virtual appliance is a distributed Event Collector appliance and requires a connection to any QRadar SIEM 16XX, 18XX, or 31XX series appliance.

### **QRadar Data Node Virtual 1400**

This virtual appliance provides retention and storage for events and flows. The virtual appliance expands the available data storage of Event Processors and Flow Processors, and also improves search performance.

**Note:** Encrypted data transmission between Data Nodes and Event Processors is not supported. The following firewall ports must be opened for Data Node communication with the Event Processor:

- Port 32006 between Data Nodes and the Event Processor appliance
- Port 32011 between Data Nodes and the Console's Event Processor

Size your QRadar Data Node Virtual 1400 appliance based on the EPS rate and data retention rules of the deployment.

Data retention policies are applied to a QRadar Data Node Virtual 1400 appliance in the same way that they are applied to stand-alone Event Processors and Flow Processors. The data retention policies are evaluated on a node-by-node basis. Criteria, such as free space, is based on the individual QRadar Data Node Virtual 1400 appliance and not the cluster as a whole.

Data Nodes can be added to the following appliances:

- Event Processor (16XX)
- Flow Processor (17XX)
- Event/Flow Processor (18XX)
- All-In-One (2100 and 31XX)

To enable all features included in the QRadar Data Node Virtual 1400 appliance, install it by using the Data Node 1400 appliance type.

### **QRadar QFlow Virtual 1299**

This virtual appliance provides the same visibility and function in your virtual network infrastructure that a QRadar QFlow Collector offers in your physical environment. The QRadar QFlow Collector virtual

appliance analyzes network behavior and provides Layer 7 visibility within your virtual infrastructure. Network visibility is derived from a direct connection to the virtual switch.

The QRadar QFlow Virtual 1299 virtual appliance supports a maximum of the following items:

- 10,000 flows per minute
- Three virtual switches, with one more switch that is designated as the management interface.

### **QRadar Vulnerability Manager Processor**

This appliance is used to process vulnerabilities within the applications, systems, and devices on your network or within your DMZ. The vulnerability processor provides a scanning component by default. If required, you can deploy more scanners, either on dedicated QRadar Vulnerability Manager managed host scanner appliances or QRadar managed hosts. For example, you can deploy a vulnerability scanner on an Event Collector or QRadar QFlow Collector.

### **QRadar Vulnerability Manager Scanner**

This appliance is used to scan for vulnerabilities within the applications, systems, and devices on your network or within your DMZ.

### **QRadar Risk Manager**

This appliance is used for monitoring device configurations, simulating changes to your network environment, and prioritizing risks and vulnerabilities in your network.

### **QRadar App Host 4000**

This appliance is a managed host that is dedicated to running apps. App Hosts provide extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your QRadar Console. Apps such as User Behavior Analytics with Machine Learning Analytics require more resources than are currently available on the Console.

### **QRadar Incident Forensics**

QRadar Incident Forensics is installed from a separate ISO than other QRadar appliances. For more information about installing QRadar Incident Forensics as a virtual appliance, see "Virtual appliance installations for QRadar Incident Forensics" in *IBM QRadar Incident Forensics Installation Guide*.

## **System requirements for virtual appliances**

---

To ensure that IBM QRadar works correctly, you must use virtual appliances that meet the minimum requirements.

For more information about supported hypervisors and virtual hardware versions, see [“Creating your virtual machine”](#) on page 24.

**Note:** The minimum requirements support QRadar functionality with minimum data sets and performance. The minimum requirements support a QRadar system that uses only the default apps. For optimal performance, use the suggested requirements.

QRadar Incident Forensics is installed from a separate ISO than other QRadar appliances. For more information about installing QRadar Incident Forensics as a virtual appliance, see "Virtual appliance installations for QRadar Incident Forensics" in *IBM QRadar Incident Forensics Installation Guide*.

### **Memory requirements**

The following table describes the memory requirements for virtual appliances.

*Table 9. Minimum and suggested memory requirements for QRadar virtual appliances*

<b>Appliance</b>	<b>Minimum memory requirement</b>	<b>Suggested memory requirement</b>
QRadar QFlow Virtual 1299	6 GB	6 GB
QRadar Data Node Virtual 1400 appliance	24 GB	48 GB
QRadar Event Collector Virtual 1599	12 GB	16 GB
QRadar SIEM Event Processor Virtual 1699 up to 20,000 EPS	12 GB	48 GB
QRadar SIEM Event Processor Virtual 1699 20,000 EPS or higher	128 GB	128 GB
QRadar SIEM Flow Processor Virtual 1799 up to 1,200,000 FPM	12 GB	48 GB
QRadar SIEM Flow Processor Virtual 1799 1,200,000 FPM or higher	128 GB	128 GB
QRadar SIEM Event and Flow Processor Virtual 1899 5,000 EPS or less 200,000 FPM or less	12 GB	48 GB
QRadar SIEM Event and Flow Processor Virtual 1899 30,000 EPS or less 1,000,000 FPM or less	128 GB	128 GB
QRadar SIEM All-in-One Virtual 3199 5,000 EPS or less 200,000 FPM or less	32 GB	48 GB
QRadar SIEM All-in-One Virtual 3199 30,000 EPS or less 1,000,000 FPM or less	64 GB	128 GB
QRadar Log Manager Virtual 8099	24 GB	48 GB
QRadar Risk Manager	24 GB	48 GB
QRadar Vulnerability Manager Processor	32 GB	32 GB

<i>Table 9. Minimum and suggested memory requirements for QRadar virtual appliances (continued)</i>		
<b>Appliance</b>	<b>Minimum memory requirement</b>	<b>Suggested memory requirement</b>
QRadar Vulnerability Manager Scanner	16 GB	16 GB
QRadar App Host	12 GB	64 GB or more for a medium sized App Host 128 GB or more for a large sized App Host

### Processor requirements

The following table describes the CPU requirements for virtual appliances.

<i>Table 10. CPU requirements for QRadar virtual appliances</i>			
<b>QRadar appliance</b>	<b>Threshold</b>	<b>Minimum number of CPU cores</b>	<b>Suggested number of CPU cores</b>
QRadar QFlow Virtual 1299	10,000 FPM or less	4	4
QRadar Event Collector Virtual 1599	2,500 EPS or less	4	16
	5,000 EPS or less	8	16
	20,000 EPS or less	16	16
QRadar SIEM Event Processor Virtual 1699	2,500 EPS or less	4	24
	5,000 EPS or less	8	24
	20,000 EPS or less	16	24
	40,000 EPS or less	40	40
	80,000 EPS or less	56	56
QRadar SIEM Flow Processor Virtual 1799	150,000 FPM or less	4	24
	300,000 FPM or less	8	24
	1,200,000 FPM or less	16	24
	2,400,000 FPM or less	48	48
	3,600,000 FPM or less	56	56
QRadar SIEM Event and Flow Processor Virtual 1899	200,000 FPM or less 5,000 EPS or less	16	24
	300,000 FPM or less 15,000 EPS or less	48	48
	1,200,000 FPM or less 30,000 EPS or less	56	56

Table 10. CPU requirements for QRadar virtual appliances (continued)

QRadar appliance	Threshold	Minimum number of CPU cores	Suggested number of CPU cores
QRadar SIEM All-in-One Virtual 3199	25,000 FPM or less 500 EPS or less	4	24
	50,000 FPM or less 1,000 EPS or less	8	24
	100,000 FPM or less 1,000 EPS or less	12	24
	200,000 FPM or less 5,000 EPS or less	16	24
	300,000 FPM or less 15,000 EPS or less	48	48
	1,200,000 FPM or less 30,000 EPS or less	56	56
QRadar Log Manager Virtual 8099	2,500 EPS or less	4	16
	5,000 EPS or less	8	16
QRadar Vulnerability Manager Processor		4	4
QRadar Vulnerability Manager Scanner		4	4
QRadar Risk Manager		8	8
QRadar Data Node Virtual 1400 appliance		4	16
QRadar App Host		4	12 or more for a medium sized App Host 24 or more for a large sized App Host

### Storage requirements

Your virtual appliance must have at least 256 GB of storage available. Before you install your virtual appliance, use QRadar: Storage Performance Requirements ([www.ibm.com/support/docview.wss?uid=swg21993402](http://www.ibm.com/support/docview.wss?uid=swg21993402)) and the spreadsheet in the *Calculating Event Storage Requirements* section of *Event FAQ* (<https://developer.ibm.com/qradar/2017/08/22/1775/>) to determine your storage needs. Use thin provisioning.

The following table shows the storage requirements for installing QRadar by using the virtual or software only option.

Table 11. Minimum storage requirements for appliances when you use the virtual or software installation option.

System classification	Appliance information	IOPS	Data transfer rate (MB/s)
Minimum performance	Supports XX05 licensing	800	500
Medium performance	Supports XX29 licensing	1200	1000
High Performance	Supports XX48 licensing	10,000	2000
Small All-in-One or 1600	Less than 500 EPS	300	300
Event/Flow Collectors	Events and flows	300	300

### Related tasks

#### Creating your virtual machine

To install a IBM QRadar virtual appliance, you must first create a virtual machine.

## Creating your virtual machine

To install a IBM QRadar virtual appliance, you must first create a virtual machine.

### Procedure

1. Create a virtual machine by using one of the following hypervisors:

- VMWare ESXi with hardware version 13
- KVM on CentOS or Red Hat Enterprise Linux 7.5 with QEMU KVM 1.5.3-141
- The Hyper-V plugin on Windows Server 2016 with all Windows updates applied

### Notes:

- If you are installing a QRadar appliance in Hyper-V, you must do a software installation, not an appliance installation. If you are using a version of Hyper-V that includes a secure boot option, secure boot must be disabled.
- If you are installing QRadar on a Unified Extensible Firmware Interface (UEFI) system, secure boot must be disabled.
- The listed hypervisor versions are tested by IBM, but other untested versions might also work. If you install QRadar on an unsupported version and encounter an issue that can be produced on the listed version of that hypervisor, IBM supports that issue.

For more information about VMWare ESXi and hardware versions, see [ESXi/ESX hosts and compatible virtual machine hardware versions list](https://kb.vmware.com/s/article/2007240) (<https://kb.vmware.com/s/article/2007240>).

2. Configure your virtual machine to meet the requirements for CPUs, RAM, and storage parameters. See [“System requirements for virtual appliances” on page 20](#).
3. Configure at least one network interface for your virtual machine.

### What to do next

[“Installing QRadar on a virtual machine” on page 25](#)

## Installing QRadar on a virtual machine

---

After you create your virtual machine, you must install the IBM QRadar software on the virtual machine.

### Before you begin

Create a virtual machine. For more information, see [“Creating your virtual machine” on page 24](#).

Determine if you need to do an appliance installation or a software installation. For more information about appliance installations and software installations, see [Chapter 3, “Virtual appliance installations,” on page 17](#).

For a software installation, you must install Red Hat Enterprise Linux (RHEL) before you install QRadar. For more information about installing RHEL for QRadar, see [“Installing RHEL on your hardware” on page 12](#).

### Procedure

1. Log in to the virtual machine by typing `root` for the user name.  
The user name is case-sensitive.
2. Accept the **End User License Agreement**.
3. Select the appliance type:
  - **Non-Software Appliance** for an appliance installation.
  - **Software Appliance** for a software installation.
4. Select the appliance assignment, and then select **Next**.
5. If you selected an appliance for high-availability (HA), select whether the appliance is a console.
6. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.
7. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
8. Select the Internet Protocol version:
  - Select **ipv4** or **ipv6**.
9. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.
10. Select the bonded interface setup, if required.
11. Select the management interface.
12. In the wizard, enter a fully qualified domain name in the **Hostname** field.
13. In the **IP address** field, enter a static IP address, or use the assigned IP address.

**Important:** If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically generated IP address. The generated IP address is entered during HA configuration.

For more information, see the *IBM Security QRadar High Availability Guide*.

14. If you do not have an email server, enter `localhost` in the **Email server name** field.
15. Enter `root` and `admin` passwords that meet the following criteria:
  - Contains at least 5 characters
  - Contains no spaces
  - Can include the following special characters: `@`, `#`, `^`, and `*`.
16. Click **Finish**.
17. Follow the instructions in the installation wizard to complete the installation.

The installation process might take several minutes. When the installation is complete, if you are installing a QRadar Console, proceed to step 18. If you are installing a managed host, proceed to [“Adding your virtual appliance to your deployment” on page 26](#).

18. Apply your license key.

a) Log in to QRadar:

`https://QRadar_IP_Address`

b) Click **Login**.

c) On the navigation menu (☰), click **Admin**.

d) In the navigation pane, click **System Configuration**.

e) Click the **System and License Management** icon.

f) From the **Display** list box, select **Licenses**, and upload your license key.

g) Select the unallocated license and click **Allocate System to License**.

h) From the list of systems, select a system, and click **Allocate System to License**.

## Adding your virtual appliance to your deployment

---

If your virtual appliance is a managed host, add your virtual appliance to your deployment.

### Procedure

1. Log in to your QRadar Console.

2. On the navigation menu (☰), click **Admin**.

3. In the **Admin** settings, click the **System and License Management** icon.

4. On the **Deployment Actions** menu, click **Add Host**.

5. Configure the settings for the managed host by providing the fixed IP address, and the root password to access the operating system shell on the appliance.

6. Click **Add**.

7. In the **Admin** settings, click **Deploy Changes**.

8. If you are installing a Console, apply your license key.

a) Log in to QRadar as the admin user:

`https://<IP_Address_QRadar>`

b) Click **Login**.

c) On the navigation menu (☰), click **Admin**.

d) In the navigation pane, click **System Configuration**.

e) Click the **System and License Management** icon.

f) From the **Display** list box, select **Licenses**, and upload your license key.

g) Select the unallocated license and click **Allocate System to License**.

h) From the list of systems, select a system, and click **Allocate System to License**.



---

## Chapter 4. Installations from the recovery partition

When you install IBM QRadar products, the installer (ISO image) is copied to the recovery partition. From this partition, you can reinstall QRadar products. Your system is restored back to the default configuration. Your current configuration and data files are overwritten.

When you restart your QRadar appliance, an option to reinstall the software is displayed. If you do not respond to the prompt within 5 seconds, the system continues to start as normal. Your configuration and data files are maintained. If you choose the reinstall option, a warning message is displayed and you must confirm that you want to reinstall.

The warning message states that you can retain the data on the appliance. This data includes events and flows. Selecting the retain option backs up the data before the reinstallation, and restores the data after installation completes. If the retain option is not available, the partition where the data resides may not be available, and it is not possible to back up and restore the data. The absence of the retain option can indicate a hard disk failure. Contact Customer Support if the retain option is not available.

**Important:** The retain option is not available on High-Availability systems. See the *IBM QRadar High Availability Guide* for information on recovering High-Availability appliances.

---

### Reinstalling from the recovery partition

You can reinstall IBM QRadar products from the recovery partition.

#### Before you begin

If your deployment includes offboard storage solutions, you must disconnect your offboard storage before you reinstall QRadar. After you reinstall, you can remount your external storage solutions. For more information about configuring offboard storage, see the *Offboard Storage Guide*.


#### Procedure

1. Restart your QRadar appliance and select **Factory re-install**.
2. Type `flatten` or `retain`.

The installer partitions and reformats the hard disk, installs the OS, and then reinstalls the QRadar product. You must wait for the `flatten` or `retain` process to complete. This process can take up to several minutes. When the process is complete, a confirmation is displayed.

3. Type `SETUP`.
4. Log in as the root user.
5. Ensure that the **End User License Agreement** (EULA) is displayed.

**Tip:** Press the Spacebar key to advance through the document.

6. For QRadar Console installations, select the **Enterprise** tuning template.
7. Follow the instructions in the installation wizard to complete the installation.
8. If you are installing a Console, apply your license key.
  - a) Log in to QRadar as the admin user:  
`https://<IP_Address_QRadar>`
  - b) Click **Login**.
  - c) On the navigation menu () , click **Admin**.
  - d) In the navigation pane, click **System Configuration**.
  - e) Click the **System and License Management** icon.

- f) From the **Display** list box, select **Licenses**, and upload your license key.
- g) Select the unallocated license and click **Allocate System to License**.
- h) From the list of systems, select a system, and click **Allocate System to License**.

---

## Chapter 5. Reinstalling QRadar from media

You can reinstall QRadar from media such as the ISO file or a USB flash drive.

### Before you begin

- \_\_\_ • Back up your data.
- \_\_\_ • On a Unified Extensible Firmware Interface (UEFI) system, remove the Grand Unified Bootloader (GRUB) entries for the existing QRadar installation from the UEFI boot loader before you reinstall QRadar.
  1. At boot time, press F1 to enter **System Configuration and Boot Management**.
  2. Select **Boot Manager**.
  3. Select **Delete Boot Option**.
  4. Check **grub**, then select **Commit Changes and Exit**.

### Procedure

1. At boot time, press F12 to enter **Boot Devices Manager**.
2. Select your installation media from the list.
3. At the prompt, type `flatten`.
4. To reinstall QRadar, follow the instructions in [“Installing a QRadar appliance”](#) on page 9.



## Chapter 6. Setting up a QRadar silent installation

Install IBM QRadar "silently," or perform an unattended installation.

### Before you begin

- You must have the QRadar ISO for the release that you want to install.
- You must install Red Hat Enterprise Linux (RHEL) V7.5 on the system where you want to install QRadar. For more information, see [Installing RHEL on your own appliance](#).
- Modify the SELINUX value in the /etc/sysconfig/selinux file to SELINUX=disabled, and restart the system.

### Procedure

1. As the root user, use SSH to log on to the host where you want to install QRadar.
2. In the root directory of the host where you want to install QRadar, create a file that is named AUTO\_INSTALL\_INSTRUCTIONS and contains the following content:

Table 12. Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO_INSTALL_INSTRUCTIONS file, but can have no value.			
Parameter	Value Required?	Description	Permitted values
force	Required	Forces the installation of the appliance despite any hardware issues.	true or false
api_auth_token	Optional	An authorization token. For more information about managing authorized services, see the <i>IBM Security QRadar Administration Guide</i> .	Authorization token
appliance_number	Optional	The identifier for the appliance	0, 3105, 1201, and so on.
appliance_oem	Required	Identifies the appliance provider.	qradar, forensics, and so on.
appliance_filter	Required	The appliance name or identifier.	vmware, na
bonding_enabled	Required.	Specifies whether you are using bonded interfaces.	true or false
bonding_interface	If using bonded interfaces, then required.	The MAC addresses for the interfaces that you are bonding, separated by commas.	<interface_name=mac_address> , <slave_interface_name=mac_address>

*Table 12. Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO\_INSTALL\_INSTRUCTIONS file, but can have no value. (continued)*

Parameter	Value Required?	Description	Permitted values
bonding_interface_name	If using bonded interfaces, then required.	Identifies the bonding interface.	bond0
bonding_options	If using bonded interfaces, then required.	The Linux options for bonded interfaces. For more information about NIC bonding, see the <i>IBM Security QRadar Administration Guide</i> .	<b>Example:</b> miimon=100 mode=4 lacp_rate=1
email_server	Required	The mail server or SMTP name, such as localhost.	
ha_cluster_virtual_ip	Optional	Specifies the IP address for the HA cluster.	ip_address
hostname	Required	The fully qualified host name for your QRadar system.	
ip_protocol	Required	The IP protocol for this host.	ipv4, ipv6
ip_dns_primary	If ip_protocol is set to IPv4, then required	The primary DNS server.	A valid IPv4 address.
ip_dns_secondary	If ip_protocol is set to IPv4, then required	The secondary DNS server.	A valid IPv4 address.
ip_management_interface	Required	The interface name, and the MAC address of the management interface. You can use either, or both separated by "=".	
ipv4_address	If ip_protocol is set to IPv4, then required	The IP address of the host that you are installing the software on.	A valid IPv4 address
ipv4_address_public	If ip_protocol is set to IPv4, and NATed, then required	The public IP address of the host that you are installing the software on.	A valid IPv4 address

*Table 12. Silent Install File parameters.* Parameters that are listed as "Optional" are required in the AUTO\_INSTALL\_INSTRUCTIONS file, but can have no value. *(continued)*

Parameter	Value Required?	Description	Permitted values
ipv4_gateway	If ip_protocol is set to IPv4, then required	The network gateway for this host	A valid IPv4 address
ipv4_network_mask	If ip_protocol is set to IPv4, then required	The netmask for this host	
ip_v6_address	If ip_protocol is set to IPv6, then required	The IPv6 address of the QRadar installation if required.	A valid IPv6 address
ip_v6_address_public	If ip_protocol is set to IPv6, and NATed, then required	The public IP address of the host that you are installing the software on.	A valid IPv6 address
ip_v6_autoconf	Required	Specifies whether IPv6 is autoconfigured.	true or false
ip_v6_gateway	Not required	Leave empty.	
is_console	Required	Specifies whether this host is the console within the deployment	true - This host is the console in the deployment false - This is not the console and is another type of managed host (Event or Flow Processor, and so on)
is_console_standby	Required.	Specifies whether this host is an HA console standby	true or false

Table 12. Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO\_INSTALL\_INSTRUCTIONS file, but can have no value. (continued)

Parameter	Value Required?	Description	Permitted values
admin_password	Optional.	The password for the administrator account. You can encrypt the password if required. If you leave this parameter blank, the password is not updated.	<p>&lt;password&gt;</p> <p><b>Important:</b> Your company's security policies can prevent you from entering a password in a static file on the appliance.</p> <p>Defined, or leaving the value empty to use a previously entered password on an upgrade.</p>
root_password	Required	The password for the root account. You can encrypt the password, if required. If you leave this parameter blank, the password is not updated.	<p>&lt;password&gt;</p> <p><b>Important:</b> Your company's security policies can prevent you from entering a password in a static file on the appliance.</p> <p>Defined, or leaving the value empty uses a previously entered password on an upgrade.</p>
security_template	If isconsole is set to Y, then required	<p>The security template</p> <p>This value must be consistent with the value entered in appliance_number.</p>	<p>Enterprise - for all SIEM-based hosts</p> <p>Logger - for Log Manager</p>
time_current_date	Required	<p>The current date for this host.</p> <p>Use the following format:</p> <p>YYYY/MM/DD format</p>	
time_current_time	Required	The time for the host in the 24 hour format HH:MM:SS.	
time_ntp_server	Optional	The FQHN or IP address of the network time protocol (NTP) server.	
timezone	Required	The time zone from the TZ database. For more information, see <a href="http://timezonedb.com/">http://timezonedb.com/</a> .	<p>Europe/London</p> <p>GMT</p> <p>America/Montreal</p> <p>America/New_York</p> <p>America/Los_Angeles</p> <p>Asia/Tokyo, and so on.</p>



*Table 12. Silent Install File parameters. Parameters that are listed as "Optional" are required in the AUTO\_INSTALL\_INSTRUCTIONS file, but can have no value. (continued)*

Parameter	Value Required?	Description	Permitted values
type_of_setup	Required	Specifies the type of installation for this host	normal- A standard QRadar managed host or console deployment.  recovery - A High Availability (HA) recovery installation on this host.
console_host	Required for SIOC	The name for your IBM QRadar on Cloud system.	IP address
Gateway setup choice	Required for SIOC	Type True if this appliance is an IBM QRadar on Cloud gateway. Type False if the appliance is not a gateway appliance.	true or false
http_proxy_host	Optional	The host name of the proxy host for the IBM QRadar on Cloud appliance.	
http_proxy_password	Optional	The password for the proxy host for the IBM QRadar on Cloud appliance.	
http_proxy_port	Optional	The identifier for the port you connect to on the proxy host for the IBM QRadar on Cloud appliance.	
http_proxy_user	Optional	The user name for the proxy host for the IBM QRadar on Cloud appliance.	
internet_access_mode	Required for SIOC	The mode that you use to access the IBM QRadar on Cloud appliance	direct or proxy

**Example:**

```
#0.0.1
ai_force=<true_false>
ai_api_auth_token= <certificate>
ai_appliance_number= <####>
ai_appliance_oem= <qradar_forensics_or_oem>
ai_appliance_filter= <appliance_number_or_identifier>
ai_bonding_enabled= <true_or_false>
ai_bonding_interfaces= <mac_address>
ai_bonding_interface_name= <interface_identifier>
ai_bonding_options= <bonding_option_identifiers>
ai_email_server= <smtp_name>
ai_gateway_setup_choice= <true_or_false>
ai_ha_cluster_virtual_ip= <IP_address>
ai_hostname= <hostname_with_FQDN>
ai_ip_dns_primary= <IP_address_of_primary_DNS>
ai_ip_dns_secondary= <IP_address_of_secondary_DNS>
ai_ip_management_interface= <MAC_address>
ai_ip_protocol= <ipv4_or_ipv6>
ai_ip_v4_address= <IP_address>
ai_ip_v4_address_public= <public_IP_address>
ai_ip_v4_gateway= <IP_address_of_gateway>
ai_ip_v4_network_mask= <network_mask>
ai_ip_v6_address= <IPv6_address>
ai_ip_v6_address_public= <IPv6_public_address>
ai_ip_v6_autoconf= <true_false>
ai_ip_v6_gateway= <IP_address>
```

```

ai_is_console= <true_or_false>
ai_is_console_standby= <true_or_false>
ai_root_password= <password_for_root_account>
ai_security_template= <enterprise_or_logger>
ai_time_current_date= <yyyy-mm-dd>
ai_time_current_time= <hh:mm:ss>
ai_time_ntp_server= <ntpserver_hostserver>
ai_timezone= <EST_or_PST_or_timezone>
ai_type_of_setup= <normal_or_recovery>
ai_console_host= <IP_address_or_identifier_for_SIOC_7000_host>
ai_http_proxy_host= <SIOC_7000_proxy_hostname>
ai_http_proxy_password= <SIOC_7000_proxy_password>
ai_http_proxy_port= <SIOC_7000_proxy_port>
ai_http_proxy_user= <SIOC_7000_proxy_user_name>
ai_internet_access_mode= <SIOC_7000_direct_or_proxy>

```

Replace the configuration settings in the file with ones that are suitable for your environment.

**Important:** Ensure that the AUTO\_INSTALL\_INSTRUCTIONS file has no extension, such as .txt, or .doc. The installation does not succeed if the file has an extension.

3. Using an SFTP program copy the QRadar ISO to the host where you want to install QRadar.
4. On the host where you are installing, create a /media/cdrom directory on the host by using the following command:

```
mkdir /media/cdrom
```

5. Mount the QRadar ISO by using the following command:

```
mount -o loop <qradar.iso> /media/cdrom
```

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

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

## Chapter 7. Overview of QRadar deployment in a cloud environment

You can install instances of IBM QRadar software on a cloud server that is hosted by a supported cloud platform. To establish secure communications between on-premises and cloud instances of QRadar, you must configure a VPN connection. You can use your cloud provider's VPN infrastructure, or configure an OpenVPN connection.

**Important:** Ensure that the following requirements are met to avoid compromised security data:

- Set a strong root password.
- Allow only specific connections to ports 443 (https), 22 (ssh), and 1194 (UDP, TCP for OpenVPN).

Configure QRadar for the cloud in the following order:

1. Install QRadar.
2. If you are using OpenVPN, determine which of your cloud and on-premises hosts is:
  - The server endpoint of a VPN tunnel. This is typically a host that is reachable by using a public IP address.
  - The client endpoint of a VPN tunnel. This is typically a host that is behind a NAT firewall.
  - The member host that routes traffic that is destined for the VPN tunnel through the local VPN endpoint.

**Note:** Your deployment can also include some hosts that have no need to communicate with hosts on the other side of the VPN tunnel.

3. Confirm that the QRadar firewall settings protect your network security.

### Configuring a QRadar host on Amazon Web Services

Configure IBM QRadar on an Amazon Web Services (AWS) instance.

#### Before you begin

1. Configure a key pair on AWS.
2. Create an Amazon EC2 instance that meets the following requirements:

Table 13. AWS Instance Requirements	
Requirement	Value
Image	RHEL - 7.5_HVM_GA-20180322-x86_64-1-Hourly2-GP2, found in <b>Community AMIs</b>
Instance type	Choose an instance that meets the <a href="#">system requirements for virtual appliances</a> .
Storage	Two disks: 1 x 100 GB volume  One volume for storage. Use the spreadsheet in the <i>Calculating Event Storage Requirements</i> section of Event FAQ ( <a href="https://developer.ibm.com/qradar/2017/08/22/1775/">https://developer.ibm.com/qradar/2017/08/22/1775/</a> ) to determine your storage needs (minimum 100 GB).

Table 13. AWS Instance Requirements (continued)	
Requirement	Value
Security Group	Your IP addresses from the list, with ports 22 and 443 open.

3. Download the AWS QRadar Install Helper script from [Fix Central](http://www.ibm.com/support/fixcentral/) (www.ibm.com/support/fixcentral/).
  - a. Go to the **Select product** tab.
  - b. Set **Product Group** to **IBM Security**.
  - c. Set **Select from IBM Security** to **IBM Security QRadar SIEM**.
  - d. Set **Installed Version** to **7.3.0** and click **Continue**.
  - e. Select **Browse for fixes** and click **Continue**.
  - f. Click **SCRIPT**.
  - g. Select the AWS QRadar Install Helper script.

The AWS instance key is required to log in to the instance with SSH.

### About this task

Keep the following items in mind as you perform this procedure:

- A high availability (HA) configuration is not supported in AWS QRadar installations.
- The command values that appear in this procedure are examples only. Command values can vary among deployments.



#### Attention:

- Do not run the **yum update** command before or after the installation. Upgrading the QRadar installation updates the operating system packages.
- Do not create partitions or do any LVM management before you run the AWS QRadar Install Helper script. The script sets up the necessary partitions.

### Procedure

1. To copy the script that prepares the AWS partitions and configuration options to the AWS instance, type the following command:

```
scp -i <key.pem> aws_qradar_prep.sh ec2-user@<public_IP_address>:
```

2. To log in to the AWS instance by using the key pair that you created when you configured the instance, type the following command:

```
ssh -i <key.pem> ec2-user@<public_IP_address>
```

3. To update dracut, type the following command:

```
yum update -y dracut
```

4. To run the script to prepare the AWS partitions and configuration options, type the following command:

```
sudo bash +x ./aws_qradar_prep.sh --install
```

The AWS instance restarts after the script runs.

5. To copy the ISO image to the device, type the following command:

```
scp -i <key.pem> <qradar.iso> ec2-user@<public_IP_address>:
```

6. To mount the ISO image, type the following command:

```
sudo mount -o loop /home/ec2-user/<qradar.iso> /media/cdrom
```

7. To copy the network configuration files to /root, type the following commands:

```
cp /etc/sysconfig/network /root
cp /etc/sysconfig/network-scripts/ifcfg-eth0 /root
```

8. To start the setup program, type the following command:

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

9. Type Y when prompted to accept an installation on unsupported hardware.
10. Follow the prompts to complete the QRadar installation wizard.

**Important:** You must specify a root password when prompted.

11. To copy the network configuration files back, type the following commands:

```
cp /root/network /etc/sysconfig
cp /root/ifcfg-eth0 /etc/sysconfig/network-scripts
```

## Configuring server endpoints for cloud installations

Use OpenVPN to configure a server endpoint on the cloud server when the IBM QRadar console is on-premises, with more processing and storage nodes are installed in the cloud.

### Before you begin

You need to know the IP addresses of your endpoints and the subnets that they'll be routing to and from.

### About this task

QRadar provides a script called `vpntool` that handles the following required items for your server endpoint:

- A main OpenVPN configuration file.
- Routing instructions for each client in the server configuration file.
- A configuration file for each client that records routing instructions for each client that can connect.
- Additional iptables rules that allow forwarding across the tunnel.
- IP forwarding enabled in the kernel.
- A custom certificate authority (CA) to issue the certificates that are used to authenticate servers and clients.
- A server certificate that is issued by the local CA.

For more information, type the following command.

```
/opt/qradar/bin/vpntool -h
```

### Procedure

1. To specify the server endpoint, type the following command to define the server endpoint.

```
/opt/qradar/bin/vpntool server <server_host_IP_address> <server_subnet_in_cidr>
```

#### Example:

```
/opt/qradar/bin/vpntool server 192.0.2.1 192.0.2.0/24
```

If your network requires TCP rather than UDP mode on your clients and servers, for example if you are using an HTTP proxy, type the following command with your required IP addresses:

```
/opt/qradar/bin/vpntool server <server_host_IP_address>  
<server_subnet_in_cidr> --tcp
```

After you define the server endpoint, VPNtool Server completes the following tasks:

- If the local certificate authority is not established, the CA is initialized and the CA key and certificate created.
- The local CA creates a key and certificate for use by this server endpoint.
- Configuration properties are written to the VPN configuration file.

2. To build and deploy the configuration, type the following command:

```
/opt/qradar/bin/vpntool deploy
```

After you build and deploy the configuration, VPNtool Server completes the following tasks:

- The OpenVPN server configuration is generated and copied into the `/etc/openvpn` directory.
- The CA certificate, and the server key and certificate, are copied into the standard location in `/etc/openvpn/pki`.
- IPtables rules are constructed and reloaded.
- IP forwarding is enabled and made persistent by updating the `/etc/sysctl.conf` file.

3. To start the server, type the following command:

```
/opt/qradar/bin/vpntool enable --now
```

Entering `/opt/qradar/bin/vpntool enable --now` creates the persistent enabled state, and automatically starts OpenVPN on system restart.

## Configuring client networks for cloud installations

In on premises environments, use OpenVPN to configure a client network that communicates with endpoints that are in the cloud.

### About this task

QRadar provides a script that is called **vpntool** that handles the following required items for your client endpoint:

- A main OpenVPN configuration file.
- Extra iptables rules to allow forwarding across the tunnel.
- IP forwarding is enabled in the kernel.
- A client certificate and the CA certificate that are issued by the CA on the VPN server endpoint.

### Procedure

1. On the server, inform the server of the new client, type the following command:

```
/opt/qradar/bin/vpntool addclient <config_name/role> <client_subnet_in_CIDR_notation>
```

#### Example:

```
/opt/qradar/bin/vpntool addclient client1 198.51.100.0/24
```

Informing the server of the client includes the following tasks:

- The CA certificate is copied to `/opt/qradar/conf/vpn/pki`.
- The client key and certificate are extracted and copied to `/opt/qradar/conf/vpn/pki`.
- Client configuration properties are written to the VPN configuration file.

2. Deploy and restart the server by using the following command:

```
/opt/qradar/bin/vpntool deploy  
systemctl restart openvpn@server
```

3. Copy the generated client credentials file and the CA file to the QRadar host that is used for this client endpoint. The files are on the system running the VPN server in the `/opt/qradar/conf/vpn/pki` directory and will be named `<config_name/role>.p12` and `ca.crt`. The files can either be copied directly to the vpn client endpoint using a tool such as **scp** or indirectly by using a USB key.

**Note:** Each client must have a unique `<config_name/role>`.

**Example:**

```
scp root@<server_IP_address>:/opt/qradar/conf/vpn/pki/ca.crt /root/ca.crt  
scp root@<server_IP_address>:/opt/qradar/conf/vpn/pki/client1.p12 /root/client1.p12
```

4. On the client, configure the host as a VPN client:

- If you are connecting the client directly to the server, type the following command:

```
/opt/qradar/bin/vpntool client <server_IP_address>  
ca.crt client1.p12
```

- If your network requires that you not configure UDP mode on your clients and servers, type the following command to use TCP:

```
/opt/qradar/bin/vpntool client <server_IP_address>  
/root/ca.crt /root/client1.p12 --tcp
```

- To connect the client through an HTTP proxy, type the following command:

```
/opt/qradar/bin/vpntool client <server_IP_address> /root/ca.crt  
/root/client1.p12 --http-proxy= <IP_address>:<port>
```

- Proxy configuration is always in TCP mode, even if you do not enter TCP in the command.
- See the OpenVPN documentation for configuration options for proxy authentication. Add these configuration options to the following file:

```
/etc/openvpn/client.conf
```

5. To build and deploy the configuration, type the following command:

```
/opt/qradar/bin/vpntool deploy
```

Building and deploying the configuration includes the following steps:

- The client OpenVPN configuration file is generated and copied into place in `/etc/openvpn`.
- The CA certificate, and client key and certificate, are copied into the standard locations within `/etc/openvpn/pki`.
- Iptables rules are generated and loaded.
- IP forwarding is enabled and made persistent by updating the `/etc/sysctl.conf` file.

6. To start the client, type the following command:

```
/opt/qradar/bin/vpntool enable --now
```

OpenVPN is in a persistent enabled state, and automatically starts on system restart.

## Configuring a member for cloud installations

---

Use OpenVPN to establish secure connections for IBM QRadar hosts that are not servers or clients, but exist in the same subnet as a server or client.

### Procedure

To join a QRadar host to the local VPN, so that it communicates directly with hosts on the other side of the tunnel, by using the following command:

```
/opt/qradar/bin/vpntool join <VPN_Server_or_Client_IP> <remote_network_CIDR_notation>
/opt/qradar/bin/vpntool deploy
```

You have an Event Processor with an IP address of 198.51.100.2 in the same subnet as a QRadar Console that is a client server. The Console has an IP address of 198.51.100.1. You want to join the Event Processor to the local VPN to communicate directly with the server host, which has an IP address of 192.0.2.0. In this example, you would type the following command:

```
/opt/qradar/bin/vpntool join 198.51.100.1 192.0.2.0/24
/opt/qradar/bin/vpntool deploy
```



---

## Chapter 8. Configuring bonded management interfaces

You can bond the management interface on QRadar hardware.

### About this task

You can bond the management interfaces during the QRadar installation process, or after installation by following these steps.

You can bond non-management interfaces in the QRadar user interface after installation. See "Configuring network interfaces" in *IBM QRadar Administration Guide* for more information about configuring non-management interfaces.

Bonding modes 1 and 4 are supported. Mode 4 is the default.

**Note:** You must be physically logged in to your appliance, for example through IMM or iDRAC, for these steps. Do not use ssh for these steps.

### Procedure

1. Change your network setup by typing the following command:

```
qchange_netsetup
```

2. Select the protocol version that is used for the appliance.
3. Select **Yes** to continue with bonded network interface configuration.
4. Select interfaces to configure as bonded interfaces. The interfaces that you select must not already be configured.
5. Enter the bonding options.  
For more information about configuring specific bonding options, see your vendor-specific operating system documentation.
6. Update any network information settings as needed.  
Your appliance restarts automatically.
7. Log in to the appliance and verify the configuration.



## Chapter 9. Network settings management

Use the `qchange_netsetup` script to change the network settings of your IBM QRadar system. Configurable network settings include host name, IP address, network mask, gateway, DNS addresses, public IP address, and email server.

### Changing the network settings in an all-in-one system

You can change the network settings in your all-in-one system. An all-in-one system has all IBM QRadar components that are installed on one system.

#### Before you begin

- You must have a local connection to your QRadar Console
- Confirm that there are no undeployed changes.
- If you are changing the IP address host name of a box in the deployment you must remove it from the deployment.
- If this system is part of an HA pair you must disable HA first before you change any network settings.
- If the system that you want to change is the console, you must remove all hosts in the deployment before proceeding.

#### Procedure

1. Log in to as the root user.
2. Type the following command:

```
qchange_netsetup
```

**Note:** If you attempt to run `qchange_netsetup` over a serial connection, the connection can be misidentified as a network connection. To run over a serial connection use `qchange_netsetup -y`. This command allows you to bypass the validation check that detects a network connection.

3. Follow the instructions in the wizard to complete the configuration.

The following table contains descriptions and notes to help you configure the network settings.

Table 14. Description of network settings for an all-in-one QRadar Console	
Network Setting	Description
Internet Protocol	IPv4 or IPv6
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	<p>Optional</p> <p>Used to access the server, usually from a different network or the Internet.</p> <p>Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).</p>

Table 14. Description of network settings for an all-in-one QRadar Console (continued)	
Network Setting	Description
Email server name	If you do not have an email server, use localhost.

A series of messages are displayed as QRadar processes the requested changes. After the requested changes are processed, the QRadar system is automatically shutdown and restarted.

## Changing the network settings of a QRadar Console in a multi-system deployment

To change the network settings in a multi-system IBM QRadar deployment, remove all managed hosts, change the network settings, add the managed hosts again, and then reassign the component.

### Before you begin


- You must have a local connection to your QRadar Console

### Procedure

- To remove managed hosts, log in to QRadar:

`https://IP_Address_QRadar`

The **Username** is admin.

- On the navigation menu () , click **Admin**.
  - Click the **System and License Management** icon.
  - Select the managed host that you want to remove.
  - Select **Deployment Actions > Remove Host**.
  - in the **Admin** settings, click **Deploy Changes**.
- Type the following command: `qchange_netsetup`.  
**Note:** If you attempt to run `qchange_netsetup` over a serial connection, the connection can be misidentified as a network connection. To run over a serial connection use `qchange_netsetup -y`. This command allows you to bypass the validation check that detects a network connection.
  - Follow the instructions in the wizard to complete the configuration.

The following table contains descriptions and notes to help you configure the network settings.

Table 15. Description of network settings for a multi-system QRadar Console deployment	
Network Setting	Description
Internet Protocol	IPv4 or IPv6
Host name	Fully qualified domain name
Secondary DNS server address	Optional


Table 15. Description of network settings for a multi-system QRadar Console deployment (continued)	
Network Setting	Description
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet.  Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).
Email server name	If you do not have an email server, use localhost.

After you configure the installation parameters, a series of messages are displayed. The installation process might take several minutes.

4. To re-add and reassign the managed hosts, log in to QRadar.


`https://IP_Address_QRadar`

The **Username** is admin.

- a) On the navigation menu () , click **Admin**.
- b) Click the **System and License Management** icon.
- c) Click **Deployment Actions > Add Host**.
- d) Follow the instructions in the wizard to add a host.

Select the **Network Address Translation** option to configure a public IP address for the server. This IP address is a secondary IP address that is used to access the server, usually from a different network or the Internet. The Public IP address is often configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. NAT translates an IP address in one network to a different IP address in another network

5. Reassign all components that are not your QRadar Console to your managed hosts .

- a) On the navigation menu () , click **Admin**.
- b) Click the **System and License Management** icon.
- c) Select the host that you want to reassign.
- d) Click **Deployment Actions > Edit Host Connection**.
- e) Enter the IP address of the source host in the **Modify Connection** window.

## Updating network settings after a NIC replacement

If you replace your integrated system board or stand-alone (Network Interface Cards) NICs, you must update your IBM QRadar network settings to ensure that your hardware remains operational.

### About this task

The network settings file contains one pair of lines for each NIC that is installed and one pair of lines for each NIC that was removed. You must remove the lines for the NIC that you removed and then rename the NIC that you installed.

**Important:** In previous releases of QRadar, interfaces were named in the following format: eth0, eth1, eth4, and so on. QRadar V7.3.1 interface naming includes a greater range of possible interface names. For example, ens192, enp2s0, and so on.

Your network settings file might resemble the following example, where *NAME*="*<old\_name>*" is the NIC that was replaced and *NAME*="*<new\_name>*" is the NIC that was installed.

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*",
ATTR{address}=="78:2a:1a:2b:3c:4d", ATTR{type}=="1",
KERNEL=="<name>*", NAME="<old_name>"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*",
ATTR{address}=="78:2a:1a:2b:3c:4d", ATTR{type}=="1",
KERNEL=="<name>*", NAME="<old_name>"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*",
ATTR{address}=="78:2a:1a:2b:3c:4d", ATTR{type}=="1",
KERNEL=="<name>*", NAME="<new_name>"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*",
ATTR{address}=="78:2a:1a:2b:3c:4d", ATTR{type}=="1",
KERNEL=="<name>*", NAME="<new_name>"
```

## Procedure

1. Use SSH to log in to the IBM QRadar product as the root user.

The user name is root.

2. Type the following command:

```
cd /etc/udev/rules.d/
```

3. To edit the network settings file, type the following command:

```
vi 70-persistent-net.rules
```

4. Remove the pair of lines for the NIC that was replaced: *NAME*="*<old\_name>*".
5. Rename the *Name*=*<name>* values for the newly installed NIC.

**Example:** Rename *NAME*="*<new\_name>*" to *NAME*="*<old\_name>*".

6. Save and close the file.
7. Type the following command: `reboot`.

## Chapter 10. Troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

Review the following table to help you or customer support resolve a problem.

Table 16. Troubleshooting actions to prevent problems	
Action	Description
Apply all known fix packs, service levels, or program temporary fixes (PTF).	A product fix might be available to fix the problem.
Ensure that the configuration is supported.	Review the software and hardware requirements.
Look up error message codes by selecting the product from the IBM Support Portal ( <a href="http://www.ibm.com/support/entry/portal">http://www.ibm.com/support/entry/portal</a> ) and then typing the error message code into the <b>Search support</b> box.	Error messages give important information to help you identify the component that is causing the problem.
Reproduce the problem to ensure that it is not just a simple error.	If samples are available with the product, you might try to reproduce the problem by using the sample data.
Check the installation directory structure and file permissions.	The installation location must contain the appropriate file structure and the file permissions.  For example, if the product requires write access to log files, ensure that the directory has the correct permission.
Review relevant documentation, such as release notes, tech notes, and proven practices documentation.	Search the IBM knowledge bases to determine whether your problem is known, has a workaround, or if it is already resolved and documented.
Review recent changes in your computing environment.	Sometimes installing new software might cause compatibility issues.

If you still need to resolve problems, you must collect diagnostic data. This data is necessary for an IBM technical-support representative to effectively troubleshoot and assist you in resolving the problem. You can also collect diagnostic data and analyze it yourself.

### Troubleshooting resources

Troubleshooting resources are sources of information that can help you resolve a problem that you have with a product. Many of the resource links provided can also be viewed in a short video demonstration.

To view the video version, search for "troubleshooting" through either Google search engine or YouTube video community.

#### Related concepts

[QRadar log files](#)

Use the IBM QRadar log files to help you troubleshoot problems.

## Support Portal

The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services.

Use IBM Support Portal to access all the IBM support resources from one place. You can adjust the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the [demo videos](https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) ([https://www.ibm.com/blogs/SPNA/entry/the\\_ibm\\_support\\_portal\\_videos](https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos)).

Find the IBM QRadar content that you need by selecting your products from the [IBM Support Portal](http://www.ibm.com/support/entry/portal) (<http://www.ibm.com/support/entry/portal>).

### Related concepts

#### [Service requests](#)

Service requests are also known as Problem Management Records (PMRs). Several methods exist to submit diagnostic information to IBM Software Technical Support.

#### [Fix Central](#)

Fix Central provides fixes and updates for your system software, hardware, and operating system.

#### [Knowledge bases](#)

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods

## Service requests

Service requests are also known as Problem Management Records (PMRs). Several methods exist to submit diagnostic information to IBM Software Technical Support.

To open a service request, or to exchange information with technical support, view the [IBM Software Support Exchanging information with Technical Support page](http://www.ibm.com/software/support/exchangeinfo.html) (<http://www.ibm.com/software/support/exchangeinfo.html>). Service requests can also be submitted directly by using the [Service requests \(PMRs\) tool](http://www.ibm.com/support/entry/portal/Open_service_request) ([http://www.ibm.com/support/entry/portal/Open\\_service\\_request](http://www.ibm.com/support/entry/portal/Open_service_request)) or one of the other supported methods that are detailed on the exchanging information page.

### Related concepts

#### [Support Portal](#)

The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services.

#### [Fix Central](#)

Fix Central provides fixes and updates for your system software, hardware, and operating system.

#### [Knowledge bases](#)

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods

## Fix Central

Fix Central provides fixes and updates for your system software, hardware, and operating system.

Use the pull-down menu to go to your product fixes on Fix Central (<http://www.ibm.com/support/fixcentral>). You might also want to view [Getting started with Fix Central](http://www.ibm.com/systems/support/fixes/en/fixcentral/help/getstarted.html) (<http://www.ibm.com/systems/support/fixes/en/fixcentral/help/getstarted.html>).

### Related concepts

#### [Support Portal](#)

The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services.

#### [Service requests](#)



Service requests are also known as Problem Management Records (PMRs). Several methods exist to submit diagnostic information to IBM Software Technical Support.

#### Knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods

#### **Related information**

Ordering PTFs Using IBM Fix Central Web Site

## **Knowledge bases**

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods

Use the following knowledge bases to find useful information.

#### **Tech notes and APARs**

From the IBM Support Portal (<http://www.ibm.com/support/entry/portal>), you can search tech notes and APARs (problem reports).

#### **IBM masthead search**

Use the IBM masthead search by typing your search string into the **Search** field at the top of any ibm.com page.

#### **External search engines**

Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com® domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

**Tip:** Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

#### **Related concepts**

##### Support Portal

The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services.

##### Service requests

Service requests are also known as Problem Management Records (PMRs). Several methods exist to submit diagnostic information to IBM Software Technical Support.

##### Fix Central

Fix Central provides fixes and updates for your system software, hardware, and operating system.

## **QRadar log files**

---

Use the IBM QRadar log files to help you troubleshoot problems.

You can review the log files for the current session individually or you can collect them to review later.

Follow these steps to review the QRadar log files.

1. To help you troubleshoot errors or exceptions, review the following log files.

- `/var/log/qradar.log`
- `/var/log/qradar.error`

2. If you require more information, review the following log files:

- `/var/log/qradar-sql.log`
- `/opt/tomcat6/logs/catalina.out`

- /var/log/qflow.debug

3. Review all logs by selecting **Admin > System & License Mgmt > Actions > Collect Log Files**.

### Related concepts

#### Troubleshooting resources

Troubleshooting resources are sources of information that can help you resolve a problem that you have with a product. Many of the resource links provided can also be viewed in a short video demonstration.

## Common ports and servers used by QRadar

---

IBM QRadar requires that certain ports are ready to receive information from QRadar components and external infrastructure. To ensure that QRadar is using the most recent security information, it also requires access to public servers and RSS feeds.

### SSH communication on port 22

All the ports that are used by the QRadar console to communicate with managed hosts can be tunneled, by encryption, through port 22 over SSH.

The console connects to the managed hosts using an encrypted SSH session to communicate securely. These SSH sessions are initiated from the console to provide data to the managed host. For example, the QRadar Console can initiate multiple SSH sessions to the Event Processor appliances for secure communication. This communication can include tunneled ports over SSH, such as HTTPS data for port 443 and Ariel query data for port 32006. IBM QRadar QFlow Collector that use encryption can initiate SSH sessions to Flow Processor appliances that require data.

### Open ports that are not required by QRadar

You might find additional open ports in the following situations:

- When you install QRadar on your own hardware, you may see open ports that are used by services, daemons, and programs included in Red Hat Enterprise Linux.
- When you mount or export a network file share, you might see dynamically assigned ports that are required for RPC services, such as `rpc.mountd` and `rpc.rquotad`.

## QRadar port usage

Review the list of common ports that IBM QRadar services and components use to communicate across the network. You can use the port list to determine which ports must be open in your network. For example, you can determine which ports must be open for the QRadar Console to communicate with remote event processors.

### WinCollect remote polling

WinCollect agents that remotely poll other Microsoft Windows operating systems might require additional port assignments.

For more information, see the IBM QRadar WinCollect *User Guide*.

### QRadar listening ports

The following table shows the QRadar ports that are open in a LISTEN state. The LISTEN ports are valid only when iptables is enabled on your system. Unless otherwise noted, information about the assigned port number applies to all QRadar products.

Table 17. Listening ports that are used by QRadar services and components

Port	Description	Protocol	Direction	Requirement
22	SSH	TCP	Bidirectional from the QRadar Console to all other components.	Remote management access.  Adding a remote system as a managed host.  Log source protocols to retrieve files from external devices, for example the log file protocol.  Users who use the command-line interface to communicate from desktops to the Console.  High-availability (HA).
25	SMTP	TCP	From all managed hosts to the SMTP gateway.	Emails from QRadar to an SMTP gateway.  Delivery of error and warning email messages to an administrative email contact.
111	Port mapper	TCP/UDP	Managed hosts that communicate with the QRadar Console.  Users that connect to the QRadar Console.	Remote Procedure Calls (RPC) for required services, such as Network File System (NFS).
123	Network Time Protocol (NTP)	UDP	Outbound from the QRadar Console to the NTP Server  Outbound from the MH to the QRadar Console	Time synchronization via Chrony between: <ul style="list-style-type: none"><li>QRadar Console and NTP server</li><li>QRadar Managed Hosts and QRadar Console</li></ul>
135 and dynamically allocated ports above 1024 for RPC calls.	DCOM	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.  Bidirectional traffic between QRadar Console components or IBM QRadar event collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.  <b>Note:</b> DCOM typically allocates a random port range for communication. You can configure Microsoft Windows products to use a specific port. For more information, see your Microsoft Windows documentation.
137	Windows NetBIOS name service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.  Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.

Table 17. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
138	Windows NetBIOS datagram service	UDP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
139	Windows NetBIOS session service	TCP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
162	NetSNMP	UDP	<p>QRadar managed hosts that connect to the QRadar Console.</p> <p>External log sources to QRadar Event Collectors.</p>	UDP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
199	NetSNMP	TCP	<p>QRadar managed hosts that connect to the QRadar Console.</p> <p>External log sources to QRadar Event Collectors.</p>	TCP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.
427	Service Location Protocol (SLP)	UDP/TCP		The Integrated Management Module uses the port to find services on a LAN.
443	Apache/HTTPS	TCP	Bidirectional traffic for secure communications from all products to the QRadar Console.	<p>Configuration downloads to managed hosts from the QRadar Console.</p> <p>QRadar managed hosts that connect to the QRadar Console.</p> <p>Users to have log in access to QRadar.</p> <p>QRadar Console that manage and provide configuration updates for WinCollect agents.</p>

Table 17. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
445	Microsoft Directory Service	TCP	<p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p>	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
514	Syslog	UDP/TCP	<p>External network appliances that provide TCP syslog events use bidirectional traffic.</p> <p>External network appliances that provide UDP syslog events use uni-directional traffic.</p> <p>Internal syslog traffic from QRadar hosts to the QRadar Console.</p>	<p>External log sources to send event data to QRadar components.</p> <p>Syslog traffic includes WinCollect agents, event collectors, and Adaptive Log Exporter agents capable of sending either UDP or TCP events to QRadar.</p>
762	Network File System (NFS) mount daemon (mountd)	TCP/UDP	Connections between the QRadar Console and NFS server.	The Network File System (NFS) mount daemon, which processes requests to mount a file system at a specified location.
1514	Syslog-ng	TCP/UDP	Connection between the local Event Collector component and local Event Processor component to the syslog-ng daemon for logging.	Internal logging port for syslog-ng.
2049	NFS	TCP	Connections between the QRadar Console and NFS server.	The Network File System (NFS) protocol to share files or data between components.
2055	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the IBM QRadar QFlow Collector.	NetFlow datagram from components, such as routers.
2375	Docker command port	TCP	Internal communications. This port is not available externally.	Used to manage QRadar application framework resources.
3389	Remote Desktop Protocol (RDP) and Ethernet over USB is enabled	TCP/UDP		If the Microsoft Windows operating system is configured to support RDP and Ethernet over USB, a user can initiate a session to the server over the management network. This means the default port for RDP, 3389 must be open.
3900	Integrated Management Module remote presence port	TCP/UDP		Use this port to interact with the QRadar console through the Integrated Management Module.

Table 17. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
4333	Redirect port	TCP		This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in QRadar offense resolution.
5000	Used to allow communication to the docker si-registry running on the Console. This allows all managed hosts to pull images from the Console that will be used to create local containers.	TCP	Unidirectional from the QRadar managed host to the QRadar Console. The port is only opened on the Console. Managed hosts must pull from the Console.	Required for apps running on an App Host.
5432	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Required for provisioning managed hosts from the <b>Admin</b> tab.
6514	Syslog	TCP	External network appliances that provide encrypted TCP syslog events use bidirectional traffic.	External log sources to send encrypted event data to QRadar components.
7676, 7677, and four randomly bound ports above 32000.	Messaging connections (IMQ)	TCP	Message queue communications between components on a managed host.	<p>Message queue broker for communications between components on a managed host.</p> <p><b>Note:</b> You must permit access to these ports from the QRadar console to unencrypted hosts.</p> <p>Ports 7676 and 7677 are static TCP ports, and four extra connections are created on random ports.</p> <p>For more information about finding randomly bound ports, see <a href="#">“Viewing IMQ port associations”</a> on page 59.</p>
7777, 7778, 7779, 7780, 7781, 7782, 7783, 7788, 7790, 7791, 7792, 7793, 7795, 7799, and 8989.	JMX server ports	TCP	Internal communications. These ports are not available externally.	<p>JMX server (Java™ Management Beans) monitoring for all internal QRadar processes to expose supportability metrics.</p> <p>These ports are used by QRadar support.</p>
7789	HA Distributed Replicated Block Device	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster.	Distributed Replicated Block Device is used to keep drives synchronized between the primary and secondary hosts in HA configurations.
7800	Apache Tomcat	TCP	From the Event Processor to the QRadar Console.	Real-time (streaming) for events.
7801	Apache Tomcat	TCP	From the Event Processor to the QRadar Console.	Real-time (streaming) for flows.
7803	Anomaly Detection Engine	TCP	From the Event Processor to the QRadar Console.	Anomaly detection engine port.
7804	QRM Arc builder	TCP	Internal control communications between QRadar processes and ARC builder.	This port is used for QRadar Risk Manager only. It is not available externally.

Table 17. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
7805	Syslog tunnel communication	TCP	Bidirectional between the QRadar Console and managed hosts	Used for encrypted communication between the console and managed hosts.
8000	Event Collection service (ECS)	TCP	From the Event Collector to the QRadar Console.	Listening port for specific Event Collection Service (ECS).
8001	SNMP daemon port	TCP	External SNMP systems that request SNMP trap information from the QRadar Console.	Listening port for external SNMP data requests.
8005	Apache Tomcat	TCP	Internal communications. Not available externally.	Open to control tomcat. This port is bound and only accepts connections from the local host.
8009	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat.	Tomcat connector, where the request is used and proxied for the web service.
8080	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat.	Tomcat connector, where the request is used and proxied for the web service.
8082	Secure tunnel for QRadar Risk Manager	TCP	Bidirectional traffic between the QRadar Console and QRadar Risk Manager	Required when encryption is used between QRadar Risk Manager and the QRadar Console.
8413	WinCollect agents	TCP	Bidirectional traffic between WinCollect agent and QRadar Console.	This traffic is generated by the WinCollect agent and communication is encrypted. It is required to provide configuration updates to the WinCollect agent and to use WinCollect in connected mode.
8844	Apache Tomcat	TCP	Unidirectional from the QRadar Console to the appliance that is running the QRadar Vulnerability Manager processor.	Used by Apache Tomcat to read RSS feeds from the host that is running the QRadar Vulnerability Manager processor.
9000	Conman	TCP	Unidirectional from the QRadar Console to a QRadar App Host.	Used with an App Host. It allows the Console to deploy apps to an App Host and to manage those apps.
9090	XForce IP Reputation database and server	TCP	Internal communications. Not available externally.	Communications between QRadar processes and the XForce Reputation IP database.
9381	Certificate files download	TCP	Unidirectional from QRadar managed host or external network to QRadar Console	Downloading QRadar CA certificate and CRL files, which can be used to validate QRadar generated certificates.
9913 plus one dynamically assigned port	Web application container	TCP	Bidirectional Java Remote Method Invocation (RMI) communication between Java Virtual Machines	When the web application is registered, one additional port is dynamically assigned.
9995	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QRadar QFlow Collector.	NetFlow datagram from components, such as routers.

Table 17. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
9999	IBM QRadar Vulnerability Manager processor	TCP	Unidirectional from the scanner to the appliance running the QRadar Vulnerability Manager processor	Used for QRadar Vulnerability Manager (QVM) command information. The QRadar Console connects to this port on the host that is running the QRadar Vulnerability Manager processor. This port is only used when QVM is enabled.
10000	QRadar web-based, system administration interface	TCP/UDP	User desktop systems to all QRadar hosts.	In QRadar V7.2.5 and earlier, this port is used for server changes, such as the hosts root password and firewall access.  Port 10000 is disabled in V7.2.6.
10101, 10102	Heartbeat command	TCP	Bidirectional traffic between the primary and secondary HA nodes.	Required to ensure that the HA nodes are still active.
12500	Socat binary	TCP	Outbound from MH to the QRadar Console	Port used for tunneling chrony udp requests over tcp when QRadar Console or MH is encrypted
15433	Postgres	TCP	Communication for the managed host that is used to access the local database instance.	Used for QRadar Vulnerability Manager (QVM) configuration and storage. This port is only used when QVM is enabled.
20000-23000	SSH Tunnel	TCP	Bidirectional from the QRadar Console to all other encrypted managed hosts.	Local listening point for SSH tunnels used for Java Message Service (JMS) communication with encrypted managed hosts. Used to perform long-running asynchronous tasks, such as updating networking configuration via System and License Management.
23111	SOAP web server	TCP		SOAP web server port for the Event Collection Service (ECS).
23333	Emulex Fibre Channel	TCP	User desktop systems that connect to QRadar appliances with a Fibre Channel card.	Emulex Fibre Channel HBAnywhere Remote Management service (elxmgmt).
32000	Normalized flow forwarding	TCP	Bidirectional between QRadar components.	Normalized flow data that is communicated from an off-site source or between QRadar QFlow Collectors.
32004	Normalized event forwarding	TCP	Bidirectional between QRadar components.	Normalized event data that is communicated from an off-site source or between QRadar Event Collectors.
32005	Data flow	TCP	Bidirectional between QRadar components.	Data flow communication port between QRadar Event Collectors when on separate managed hosts.



Table 17. Listening ports that are used by QRadar services and components (continued)

Port	Description	Protocol	Direction	Requirement
32006	Ariel queries	TCP	Bidirectional between QRadar components.	Communication port between the Ariel proxy server and the Ariel query server.
32007	Offense data	TCP	Bidirectional between QRadar components.	Events and flows contributing to an offense or involved in global correlation.
32009	Identity data	TCP	Bidirectional between QRadar components.	Identity data that is communicated between the passive Vulnerability Information Service (VIS) and the Event Collection Service (ECS).
32010	Flow listening source port	TCP	Bidirectional between QRadar components.	Flow listening port to collect data from QRadar QFlow Collectors.
32011	Ariel listening port	TCP	Bidirectional between QRadar components.	Ariel listening port for database searches, progress information, and other associated commands.
32000-33999	Data flow (flows, events, flow context)	TCP	Bidirectional between QRadar components.	Data flows, such as events, flows, flow context, and event search queries.
40799	PCAP data	UDP	From Juniper Networks SRX Series appliances to QRadar.	Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances.  <b>Note:</b> The packet capture on your device can use a different port. For more information about configuring packet capture, see your Juniper Networks SRX Series appliance documentation.
ICMP	ICMP		Bidirectional traffic between the secondary host and primary host in an HA cluster.	Testing the network connection between the secondary host and primary host in an HA cluster by using Internet Control Message Protocol (ICMP).

## Viewing IMQ port associations

Several ports that are used by IBM QRadar allocate extra random port numbers. For example, Message Queues (IMQ) open random ports for communication between components on a managed host. You can view the random port assignments for IMQ by using telnet to connect to the local host and doing a lookup on the port number.

Random port associations are not static port numbers. If a service is restarted, the ports that are generated for the service are reallocated and the service is provided with a new set of port numbers.

### Procedure

1. Using SSH, log in to the QRadar Console as the root user.
2. To display a list of associated ports for the IMQ messaging connection, type the following command:

```
telnet localhost 7676
```

The results from the telnet command might look similar to this output:

```
[root@domain ~]# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
101 imqbroker 4.4 Update 1
portmapper tcp PORTMAPPER 7676
[imqvarhome=/opt/openmq/mq/var,imqhome=/opt/openmq/mq,sessionid=<session_id>]
cluster_discovery tcp CLUSTER_DISCOVERY 44913
jmxrmi rmi JMX 0 [url=service:jmx:rmi://domain.ibm.com/stub/<urlpath>]
admin tcp ADMIN 43691
jms tcp NORMAL 7677
cluster tcp CLUSTER 36615
```

The telnet output shows 3 of the 4 random high-numbered TCP ports for IMQ. The fourth port, which is not shown, is a JMX Remote Method Invocation (RMI) port that is available over the JMX URL that is shown in the output.

If the telnet connection is refused, it means that IMQ is not currently running. It is probable that the system is either starting up or shutting down, or that services were shut down manually.

## Searching for ports in use by QRadar

Use the **netstat** command to determine which ports are in use on the IBM QRadar Console or managed host. Use the **netstat** command to view all listening and established ports on the system.

### Procedure

1. Using SSH, log in to your QRadar Console, as the root user.
2. To display all active connections and the TCP and UDP ports on which the computer is listening, type the following command:

```
netstat -nap
```

3. To search for specific information from the netstat port list, type the following command:

```
netstat -nap | grep port
```

### Examples:

- To display all ports that match 199, type the following command:

```
netstat -nap | grep 199
```

- To display information on all listening ports, type the following command:

```
netstat -nap | grep LISTEN
```

## QRadar public servers

To provide you with the most current security information, IBM QRadar requires access to a number of public servers and RSS feeds.

### Public servers

Table 18. Public servers that QRadar must access. This table lists descriptions for the IP addresses or host names that QRadar accesses.	
IP address or hostname	Description
194.153.113.31	IBM QRadar Vulnerability Manager DMZ scanner
194.153.113.32	QRadar Vulnerability Manager DMZ scanner

*Table 18. Public servers that QRadar must access.* This table lists descriptions for the IP addresses or host names that QRadar accesses. (continued)

IP address or hostname	Description
qmmunity.q1labs.com	QRadar auto-update servers. For more information about auto-update servers, see <a href="http://www.ibm.com/support">www.ibm.com/support</a> ( <a href="http://www-01.ibm.com/support/docview.wss?uid=swg21958881">http://www-01.ibm.com/support/docview.wss?uid=swg21958881</a> ).
qmmunity-eu.q1labs.com	QRadar auto-update servers. For more information about auto-update servers, see <a href="http://www.ibm.com/support">www.ibm.com/support</a> ( <a href="http://www-01.ibm.com/support/docview.wss?uid=swg21958881">http://www-01.ibm.com/support/docview.wss?uid=swg21958881</a> ).
update.xforce-security.com	X-Force® Threat Feed update server
license.xforce-security.com	X-Force Threat Feed licensing server

### RSS feeds for QRadar products

*Table 19. RSS feeds .* The following list describes the requirements for RSS feeds that QRadar uses. Copy URLs into a text editor and remove page breaks before pasting into a browser.

Title	URL	Requirements
Security Intelligence	<a href="http://feeds.feedburner.com/SecurityIntelligence">http://feeds.feedburner.com/SecurityIntelligence</a>	QRadar and an Internet connection
Security Intelligence Vulns / Threats	<a href="http://securityintelligence.com/topics/vulnerabilities-threats/feed">http://securityintelligence.com/topics/vulnerabilities-threats/feed</a>	QRadar and an Internet connection
IBM My Notifications	<a href="http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid=feeder.create_feed&amp;feeder.feedtype=RSS&amp;feeder.uid=270006EH0R&amp;feeder.subscrid=S14b5f284d32&amp;feeder.subdefkey=swgothor&amp;feeder.maxfeed=25">http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid=feeder.create_feed&amp;feeder.feedtype=RSS&amp;feeder.uid=270006EH0R&amp;feeder.subscrid=S14b5f284d32&amp;feeder.subdefkey=swgothor&amp;feeder.maxfeed=25</a>	QRadar and an Internet connection
Security News	<a href="http://IP_address_of_QVM_processor:8844/rss/research/news.rss">http://IP_address_of_QVM_processor:8844/rss/research/news.rss</a>	IBM QRadar Vulnerability Manager processor is deployed
Security Advisories	<a href="http://IP_address_of_QVM_processor:8844/rss/research/advisories.rss">http://IP_address_of_QVM_processor:8844/rss/research/advisories.rss</a>	QRadar Vulnerability Manager processor is deployed
Latest Published Vulnerabilities	<a href="http://IP_address_of_QVM_processor:8844/rss/research/vulnerabilities.rss">http://IP_address_of_QVM_processor:8844/rss/research/vulnerabilities.rss</a>	QRadar Vulnerability Manager processor deployed
Scans Completed	<a href="http://IP_address_of_QVM_processor:8844/rss/scanresults/completedScans.rss">http://IP_address_of_QVM_processor:8844/rss/scanresults/completedScans.rss</a>	QRadar Vulnerability Manager processor is deployed
Scans In Progress	<a href="http://IP_address_of_QVM_processor:8844/rss/scanresults/runningScans.rss">http://IP_address_of_QVM_processor:8844/rss/scanresults/runningScans.rss</a>	QRadar Vulnerability Manager processor is deployed



---

## Chapter 11. Receiving QRadar update notifications

Sign up to stay informed of critical IBM software support updates.

### Procedure

1. Go to [Stay up to date - IBM Support](http://ibm.biz/MyNotification) (<http://ibm.biz/MyNotification>).
2. Click **Subscribe now!**.
3. Sign in with your IBMid.
4. Enter QRadar in the **Product lookup** field.
5. Click **Subscribe** to choose which product you want to receive notifications for.
6. Select the notifications that you want to receive.



## 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://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](http://www.ibm.com/legal/copytrade.shtml).

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

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>.

## 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>



