

IBM Security QRadar SIEM  
Version 7.1.0 MR1

*User Guide*



**Note:** Before using this information and the product that it supports, read the information in [“Notices and Trademarks”](#) on [page 21](#).

# CONTENTS

---

## ABOUT THIS GUIDE

Intended Audience . . . . .	1
Documentation Conventions . . . . .	1
Technical Documentation . . . . .	1
Contacting Customer Support . . . . .	2

---

## 1 PREPARING FOR YOUR UPGRADE

Before You Upgrade . . . . .	3
Preparing to Upgrade . . . . .	5
Pretesting Your System . . . . .	6

---

## 2 UPGRADING QRADAR SIEM

Upgrading QRadar SIEM Appliances . . . . .	9
Upgrading QRadar SIEM Software Running on Your Own Hardware . . . . .	12
Clearing the Cache . . . . .	19
Notices . . . . .	21
Trademarks . . . . .	23

---

## INDEX



# ABOUT THIS GUIDE

This guide provides information on how to upgrade your IBM Security QRadar SIEM systems to QRadar SIEM 7.1 (MR1).

---

**Intended Audience** The *IBM Security QRadar SIEM Upgrade Guide* is intended for system administrators responsible for upgrading QRadar SIEM systems.

---

**Documentation Conventions** The following conventions are used throughout this guide:

- ▶ Indicates that the procedure contains a single instruction.

**NOTE** Indicates that the information provided is supplemental to the associated feature or instruction.



**CAUTION**

*Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*



**WARNING**

*Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

---

**Technical Documentation**

For information on how to access more technical documentation, technical notes, and release notes, see the [Accessing IBM Security QRadar SIEM Documentation Technical Note](http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).  
(<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644>)

---

**Contacting  
Customer Support**

For information on contacting customer support, see the *Support and Download Technical Note*.  
(<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>)

# 1

## PREPARING FOR YOUR UPGRADE

Before you upgrade, we recommend that you review the information in this section and pretest your system. Preparing for your upgrade should prevent issues from occurring during the upgrade.

This guide includes the following topics:

- [Before You Upgrade](#)
- [Preparing to Upgrade](#)
- [Pretesting Your System](#)

---

### Before You Upgrade

Before you upgrade, you must verify your deployment meets the following requirements:

- To upgrade to QRadar SIEM 7.1.0 (MR1), you must be using QRadar SIEM 7.0 MR5. If you are not using QRadar SIEM 7.0 MR5, download and install QRadar SIEM 7.0 MR5 from the Qmmunity website. In the QRadar SIEM user interface, click **Help > About** to view your QRadar SIEM version information.
- If you are using QRadar SIEM 7.1, you must perform a fresh installation of QRadar SIEM 7.1.0 (MR1) because you cannot upgrade to QRadar SIEM 7.1.0 (MR1) patch directly from QRadar SIEM 7.1. If you attempt to upgrade, your upgrade will fail. For more information on installing QRadar SIEM 7.1.0 (MR1), see the QRadar SIEM 7.1.0 (MR1) Release Notes.
- We require that you upgrade all of the systems in your deployment to QRadar SIEM 7.1.0 (MR1).
- Close all open QRadar SIEM sessions to avoid access errors in your log file.
- Appliances cannot upgrade if they do not meet the minimum memory requirements, as specified in the following table:

**Table 1-1** Appliance Memory Requirements

Appliance	Minimum Memory Requirement	Recommended Memory Requirement
QFlow 1201	6 GB	6 GB
QFlow 1202	6 GB	6 GB

**Table 1-1** Appliance Memory Requirements (continued)

Appliance	Minimum Memory Requirement	Recommended Memory Requirement
QFlow 1301	6 GB	6 GB
QFlow 1310	6 GB	6 GB
QRadar 1501	6 GB	6 GB
QRadar 1601	8 GB	24 GB
QRadar 1605	8 GB	24 GB
QRadar 1624	8 GB	24 GB
QRadar 1601	8 GB	24 GB
QRadar 1705	8 GB	24 GB
QRadar 1724	8 GB	24 GB
QRadar 1805	8 GB	24 GB
QRadar 2100	8 GB	24 GB
QRadar 3100	8 GB	24 GB
QRadar 3105	8 GB	24 GB
QRadar 3124	8 GB	24 GB

- If you plan to enable payload indexing, we strongly recommend that your system include a minimum of 24 GB of memory.
- If you install IBM Security QRadar SIEM software on your own hardware, your system must include a minimum of 24 GB of memory.
- Any IBM Security QFlow Collector appliance with less than a 80 GB hard drive must use a fresh installation to use the latest software. For more information, see the *IBM Security QRadar SIEM Installation Guide*.
- The Java™ Runtime Environment, version 1.6.0\_u24, must be installed on the desktop system that you use to view the QRadar SIEM user interface.
- If you intend to install QRadar Risk Manager, Adobe Flash 10.x must be installed on the desktop system that you use to view the QRadar SIEM user interface.
- The IBM Security QRadar SIEM 7.1.0 (MR1) upgrade requires the following minimum free disk space:

**Table 1-2** Free Space Requirements

Partition	Free Space Requirement
/	3 GB
/store	4 GB
/var/log	500 MB
/store/tmp	800 MB



---

## Preparing to Upgrade

You must complete the upgrade process on your QRadar SIEM Console first and you must be able to access the QRadar SIEM user interface on your desktop system before upgrading your secondary Console and other systems in your deployment.

Upgrade your QRadar SIEM systems in the following order:

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

If you are upgrading QRadar SIEM systems in an HA deployment, you must upgrade the primary system before upgrading the associated secondary system. The primary host must be the active system in your deployment. If the secondary host is the active system, the upgrade of the primary host to QRadar SIEM 7.1.0 (MR1) cancels. For more information on managing HA, see the *IBM Security QRadar SIEM Administration Guide*.



---

### CAUTION

*If you are upgrading QRadar systems in an HA deployment that is configured with an offboard storage solution, you must first disconnect the HA pair, upgrade the primary system to QRadar 7.1, install QRadar 7.1 fresh on the associated secondary system, reconfigure external storage on both HA systems, and then reconnect the HA pair. For more information on reconnecting your offboard storage solutions, see the *Reconfiguring Offboard Storage During an Upgrade to QRadar 7.1.0 (MR1)*.*

---



---

### CAUTION

*Disk replication and failovers are disabled until the primary and secondary hosts synchronize and the **needs upgrade** or **failed** status is cleared from the secondary host.*

---

During the upgrade of a secondary host, the System and License Management screen changes the status of the secondary host to **upgrading**. After the upgrade of the secondary host is complete, you may need to restore the configuration of the secondary host. For more information on restoring a failed host, see the *IBM Security QRadar SIEM Administration Guide*.

If you are upgrading the QRadar SIEM software installed on your own appliance, ensure that you have one of the following portable storage devices:

- Digital Versatile Disk (DVD)
- Bootable USB flash-drive

If your deployment consists of a virtual appliance and you have questions concerning your deployment, contact Customer Support for assistance. For information on QRadar appliances and hardware, see the *QRadar Hardware Installation Guide*.

---

## Pretesting Your System

Before you upgrade to QRadar SIEM 7.1.0 (MR1), perform a pretest on all the systems in your deployment to ensure that your deployment meets the requirements for the upgrade. We recommend that you schedule the pretest during non-peak hours.

The output of the pretest determines if your system meets the upgrade system requirements, such as:

- Memory requirements
- Partitioning
- Supported and required RPMs
- Log source limits
- Licensing
- Out of memory notifications
- Disk sentry notifications
- Invalid passwords
- Failed logins
- PostgreSQL issues
- Table constraint/key issues

Third-party RPMs are not supported on QRadar SIEM systems. If the pretest discovers unsupported RPMs, remove the unsupported RPMs before upgrading your system. If the pretest discovers that required RPMs have been removed, you must re-install the required RPMs before continuing with your upgrade.

To pretest your QRadar SIEM system:

**Step 1** Using SSH, log in to QRadar SIEM as the root user.

Username: **root**

Password: **<password>**

**Step 2** Choose one of the following:

- If you are upgrading a Console, go to [Step 3](#).
- If you are upgrading a managed host, go to [Step 4](#).

- If you are upgrading a secondary HA host, go to **Step 5**.

**Step 3** Download and mount the QRadar SIEM 7.1.0 (MR1) software:

- a Create the /store/iso folder by typing the following command:

```
mkdir /store/iso
```

- b Go to the Qmmunity website to access the QRadar SIEM 7.1.0 (MR1) download:

```
https://qmmunity.qllabs.com/products/
```

- c Copy the file to the /store/iso folder on your system.

- d Mount the ISO by typing the following command:

```
mount -o loop /store/iso/<ISO file name> /media/cdrom
```



### CAUTION

---

*Ensure that there are no CDs in the disk drive before you proceed.*

---

Go to **Step 6**.

**Step 4** Copy the QRadar SIEM 7.1.0 (MR1) ISO from the Console and mount the ISO:

- a Create the /store/iso folder by typing the following:

```
mkdir /store/iso
```

- b Using SSH, log in to your Console as the root user:

Username: **root**

Password: **<password>**

- c Copy the QRadar SIEM 7.1.0 (MR1) ISO to the /store/iso folder on your system:

```
scp <ISO file name> <ip_address>:/store/iso
```

Where **<ip\_address>** is the IP address of the managed host.

- d Using SSH, log in to your managed host as the root user:

Username: **root**

Password: **<password>**

- e Mount the QRadar SIEM 7.1.0 (MR1) ISO by typing the following command:

```
mount -o loop /store/iso/<ISO file name> /media/cdrom
```



### CAUTION

---

*Ensure that there are no CDs in the disk drive before you proceed.*

---

Go to **Step 6**.

**Step 5** Download and mount the QRadar SIEM 7.1.0 (MR1) software for secondary HA systems:

- a Go to the Qmmunity website to access the QRadar SIEM 7.1.0 (MR1) download:  
`https://qmmunity.q11labs.com/products/`
- b Copy the file to the / folder on your system.
- c Mount the ISO by typing the following command:  
`mount -o loop /<ISO file name> /media/cdrom`

**CAUTION**


---

*Ensure that there are no CDs in the disk drive before you proceed.*

---

- Step 6** Perform the pretest by typing the following:

```
/media/cdrom/setup -t
```

The following message is displayed:

```
About to run pretests in preparation for upgrade from version
7.1.0.<Build version> to 7.1.0.<Build version>
Do you wish to continue (Y/[N])?
```

- Step 7** Type **y** to continue the pretest.

**CAUTION**


---

*When pretesting your system, you are prompted to run PRETESTDOWN scripts after the initial PRETEST is complete. The PRETESTDOWN scripts require all services to be stopped to test the integrity of the database, resulting in a data outage.*

---

The following message is displayed:

```
Completed all PRETEST scripts successfully.
***** WARNING *****
About to run PRETESTDOWN scripts which will cause tomcat and
hostcontext services to be stopped and cause a data outage.
These test scripts will be run:
check_db_upgrade.sh
check_permissions.sh
ha_shutdown.sh
***** WARNING *****
Proceed (Y/[N]) (default to N after 55 seconds)?
Are you absolutely sure? THERE WILL BE A DATA OUTAGE!
Proceed (Y/[N]) (default to N after 50 seconds)?
```

- Step 8** Type **y** to run the PRETESTDOWN scripts.

If the pretest indicates a problem, contact Customer Support.

# 2

## UPGRADING QRADAR SIEM

IBM Security QRadar SIEM appliances now run on the Red Hat Enterprise Linux operating system. When you upgrade a QRadar SIEM appliance that previously ran the CentOS operating system, the upgrade script removes CentOS and installs Red Hat Enterprise Linux 6.3 on your appliance. When you upgrade an appliance that used a previous Red Hat Enterprise Linux version, the upgrade script requires you to install and configure Red Hat Enterprise Linux 6.3 on your appliance.

This section includes the following topics:

- [Upgrading QRadar SIEM Appliances](#)
- [Upgrading QRadar SIEM Software Running on Your Own Hardware](#)
- [Clearing the Cache](#)

---

### Upgrading QRadar SIEM Appliances

When you upgrade your QRadar SIEM appliance to QRadar SIEM 7.1.0 (MR1), the CentOS operating system is replaced by Red Hat Enterprise Linux. The upgrade procedure may take an extended period of time to complete. Ensure that you backup your data before you begin any software upgrade. For more information on backup and recovery, see the *IBM Security QRadar SIEM Administration Guide*.



#### CAUTION

---

*If your deployment includes offboard storage solutions, you must remount your external storage solutions when prompted during the upgrade to QRadar SIEM 7.1.0 (MR1). For more information on configuring off-board storage, see the *Configuring Offboard Storage Guide*.*

---

We recommend that you move any unsupported data from the root directory before you upgrade. During the upgrade, the following items are removed from the system:

- Non-QRadar SIEM user accounts
- Data associated with non-QRadar SIEM user accounts
- Non-QRadar SIEM data stored in the root directory

To upgrade your appliances to QRadar SIEM 7.1.0 (MR1):

**Step 1** Using SSH, log in to QRadar SIEM as the root user.

Username: **root**

Password: **<password>**

If you pretested your system as recommended, the ISO is already downloaded and mounted. Go to **Step 6**.

**Step 2** Choose one of the following:

- If you are upgrading a Console, go to **Step 3**.
- If you are upgrading a managed host, go to **Step 4**.
- If you are upgrading a secondary HA host, go to **Step 5**.

**Step 3** Download and mount the QRadar SIEM 7.1.0 (MR1) ISO:

a Create the /store/iso folder by typing the following:

```
mkdir /store/iso
```

b Obtain the QRadar SIEM 7.1.0 (MR1) download:

- Using your web browser, go to the Qmmunity website to access the QRadar SIEM 7.1.0 (MR1) download:

```
https://qmmunity.q1labs.com/products/
```

- Copy the QRadar SIEM 7.1.0 (MR1) ISO to the /store/iso folder on your system.

c Mount the QRadar SIEM 7.1.0 (MR1) ISO by typing the following command:

```
mount -o loop /store/iso/<ISO file name> /media/cdrom
```

Go to **Step 6**.

**Step 4** Copy the QRadar SIEM 7.1.0 (MR1) ISO from the Console and mount the ISO:

a Create the /store/iso folder by typing the following:

```
mkdir /store/iso
```

b Using SSH, log in to your Console as the root user:

Username: **root**

Password: **<password>**

c Copy the QRadar SIEM 7.1.0 (MR1) ISO to the /store/iso folder on your system:

```
scp <ISO file name> <ip_address>:/store/iso
```

Where **<ip\_address>** is the IP address of the managed host.

d Using SSH, log in to your managed host as the root user:

Username: **root**

Password: **<password>**

e Mount the QRadar SIEM 7.1.0 (MR1) ISO by typing the following command:

```
mount -o loop /store/iso/<ISO file name> /media/cdrom
```

Go to **Step 6**.

**Step 5** Download and mount the QRadar SIEM 7.1.0 (MR1) ISO for secondary HA systems:

- a** Obtain the QRadar SIEM 7.1.0 (MR1) download:
- Using your web browser, go to the Qmmunity website to access the QRadar SIEM 7.1.0 (MR1) download:

```
https://qmmunity.q11labs.com/products/
```

- Copy the QRadar SIEM 7.1.0 (MR1) ISO to the / folder on your system.

**b** Mount the QRadar SIEM 7.1.0 (MR1) ISO by typing the following command:

```
mount -o loop /<ISO file name> /media/cdrom
```

**Step 6** Type the following setup command:

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

#### NOTE

---

If your system has multiple volumes and a DRAC card, the following message is displayed, indicating that the upgrade process might cancel due to an unsupported configuration: `ERROR: Upgrade on systems without sda drive not supported` or `ERROR: Upgrade on PowerEdge 2950 only supported on single RAID 10 logical disk`. If this error is displayed, contact Customer Support.

---

The End User License Agreement (EULA) is displayed.

**Step 7** Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The following prompt is displayed:

```
About to upgrade from 7.0.0-<build> to 7.1.0-<build>. Do you
wish to continue (Y/[N])?
```

**Step 8** Type **y** to continue.

The upgrade script runs a pretest to ensure your configuration meets the requirements for upgrading to QRadar SIEM 7.1.0 (MR1). If the pretest encounters issues, information messages are displayed that may require your input. Answer any prompts that are displayed to continue the pretest.

When the pretest is complete, the following message is displayed:

The upgrade process has four phases:

1. Pretest checks (Completed)
2. Upgrade data and configuration settings (Next)
3. Install Red Hat Enterprise Linux 6
4. Install new software version with upgraded data

```
Would you like to automatically restart your system at the end
of the phase 2? (Y/N)
```

**Step 9** Type `y` to continue the upgrade.

**NOTE**

If you type `n` to indicate that you do not want to automatically restart your system at the end of phase 2, you are required to manually restart your system when the upgrade prompts you.

Phase 2 of the upgrade is now in progress. Depending on your system, phase 2 can take several minutes to complete. The upgrade might prompt you to delete patch files that are no longer required by the system to save storage space.



**CAUTION**

*You must not cancel or turn off the appliance when an upgrade is in progress.*

When the phase 2 upgrade is complete, your system is automatically restarted. The following message is displayed:

```
Upgrade phase is now complete. Please reboot to initiate the
install phase.
You have new mail in /var/spool/mail/root
Please reboot your system to complete the upgrade
The upgrade portion has completed. Performing automatic reboot
as requested.
See log /var/log/setup-7.1.0.<build>/qradar_setup.log for
status.
```

**Step 10** Using SSH, log in to QRadar SIEM as the root user.

Username: **root**

Password: **<password>**



**CAUTION**

*If the upgrade script detects that your system is configured with an off-board storage solution, you are prompted to remount your off-board storage device. For instruction on how to reconfigure off-board storage, see the [Reconfiguring Offboard Storage During an Upgrade to QRadar SIEM 7.1.0 \(MR1\) Technical Note](#).*

Your upgrade is complete. The following message is displayed:

```
This server was upgraded to QRadar 7.1.0 Release <build> on
<date>.
```

## Upgrading QRadar SIEM Software Running on Your Own Hardware

When you upgrade your own appliance to QRadar SIEM 7.1.0 (MR1), the Red Hat Enterprise Linux is updated to version 6.3. The upgrade procedure may take an extended period of time to complete. Ensure that you backup your data before you begin any software upgrade. For more information on backup and recovery, see the *IBM Security QRadar SIEM Administration Guide*.



**CAUTION**


---

*If your deployment includes offboard storage solutions, you must remount your external storage solutions when prompted during the upgrade to QRadar SIEM 7.1.0 (MR1). For more information on configuring off-board storage, see the [Configuring Offboard Storage Guide](#).*

---

We recommend that you move any unsupported data from the root directory before you upgrade. During the upgrade, the following items are removed from the system:

- Non-QRadar SIEM user accounts
- Data associated with non-QRadar SIEM user accounts
- Non-QRadar SIEM data stored in the root directory

We recommend that you verify your command-line package management utility Yellowdog Updater, Modified (YUM) is configured properly, because QRadar SIEM software requires specific versions of some libraries.

To upgrade your appliances to QRadar SIEM 7.1.0 (MR1):

**Step 1** Using SSH, log in to QRadar SIEM as the root user.

Username: **root**

Password: **<password>**

If you pretested your system as recommended, the ISO is already downloaded and mounted. Go to [Step 6](#).

**Step 2** Choose one of the following:

- If you are upgrading a Console, go to [Step 3](#).
- If you are upgrading a managed host, go to [Step 4](#).
- If you are upgrading a secondary HA host, go to [Step 5](#).

**Step 3** Download and mount the QRadar SIEM 7.1.0 (MR1) ISO:

**a** Create the /store/iso folder by typing the following:

```
mkdir /store/iso
```

**b** Obtain the QRadar SIEM 7.1.0 (MR1) download:

- Using your web browser, go to the Qmmunity website to access the QRadar SIEM 7.1.0 (MR1) download:

```
https://qmmunity.q11labs.com/products/
```

- Copy the QRadar SIEM 7.1.0 (MR1) ISO to the /store/iso folder on your system.

**c** Mount the QRadar SIEM 7.1.0 (MR1) ISO by typing the following command:

```
mount -o loop /store/iso/<ISO file name> /media/cdrom
```

Go to [Step 6](#).

- Step 4** Copy the QRadar SIEM 7.1.0 (MR1) ISO from the Console and mount the ISO:
- a Create the /store/iso folder by typing the following:
 

```
mkdir /store/iso
```
  - b Using SSH, log in to your Console as the root user:
 

```
Username: root
Password: <password>
```
  - c Copy the QRadar SIEM 7.1.0 (MR1) ISO to the /store/iso folder on your system:
 

```
scp <ISO file name> <ip_address>:/store/iso
```

 Where `<ip_address>` is the IP address of the managed host.
  - d Using SSH, log in to your managed host as the root user:
 

```
Username: root
Password: <password>
```
  - e Mount the QRadar SIEM 7.1.0 (MR1) ISO by typing the following command:
 

```
mount -o loop /store/iso/<ISO file name> /media/cdrom
```

 Go to [Step 6](#).
- Step 5** Download and mount the QRadar SIEM 7.1.0 (MR1) ISO for secondary HA systems:
- a Obtain the QRadar SIEM 7.1.0 (MR1) download:
    - Using your web browser, go to the Qmmunity website to access the QRadar SIEM 7.1.0 (MR1) download:
 

```
https://qmmunity.qllabs.com/products/
```
    - Copy the QRadar SIEM 7.1.0 (MR1) ISO to the / folder on your system.
  - b Mount the QRadar SIEM 7.1.0 (MR1) ISO by typing the following command:
 

```
mount -o loop /<ISO file name> /media/cdrom
```
- Step 6** Type the following setup command:
- ```
/media/cdrom/setup
```

#### NOTE

---

If your system has multiple volumes and a DRAC card, the following message is displayed, indicating that the upgrade process might cancel due to an unsupported configuration: `ERROR: Upgrade on systems without sda drive not supported OR ERROR: Upgrade on PowerEdge 2950 only supported on single RAID 10 logical disk.` If this error is displayed, contact Customer Support.

---

The End User License Agreement (EULA) is displayed.

- Step 7** Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type `yes` to accept the agreement, and then press Enter.

The following prompt is displayed:

```
About to upgrade from 7.0.0-<build> to 7.1.0-<build>. Do you
wish to continue (Y/[N])?
```

**Step 8** To continue, type **y**.

The upgrade script runs a pretest to ensure your configuration meets the requirements for upgrading to QRadar SIEM 7.1.0 (MR1). If the pretest encounters issues, information messages are displayed that may require your input. Answer any prompts that are displayed to continue the pretest.

The following message is displayed:

```
Please reboot into the RedHat 6.3 DVD and follow the QRadar
Upgrade Documentation.

Completed all POST scripts successfully.
*****

Please reboot your system to complete the upgrade
Please reboot into the RedHat 6.3 DVD and follow the QRadar
Upgrade Documentation.

See log /var/log/setup-7.1.0.356878/qradar_setup.log for status
```

**Step 9** Install Red Hat Enterprise Linux 6.3:

- a Obtain Red Hat Enterprise Linux 6.3 DVD ISO and copy the ISO to one of the following portable storage devices:
  - Digital Versatile Disk (DVD)
  - Bootable USB flash-drive

For instructions on how to create a bootable USB flash-drive, see the *Installing QRadar Using a Bootable USB Flash-Drive Technical Note*.
- b Insert the portable storage device into your appliance.
- c Restart your appliance.
- d To load the boot menu, press the F11 or the Escape key on your keyboard.
- e Select USB drive or DVD drive as the boot option.



**CAUTION**

---

*If you are installing the Red Hat Enterprise Linux operating system on a system that supports Extensible Firmware Interface (EFI), you must start the system in legacy mode.*

---

- f When the login prompt is displayed, log in to the system as the root user. The Welcome page of the installation wizard is displayed.

**Step 10** To prevent an issue with ethernet interface address naming, perform the following steps:

- a Press the Tab key.

- b Locate the following line:

```
Vmlinuz initrd=initrd.image
```

- c At the end of the `Vmlinuz initrd=initrd.image` line, add the following text:

```
biosdevname=0
```

- d To return to the installation wizard, press Enter.

**Step 11** Click **Next** to advance to the next page.

**Step 12** Select the language that you want to use during the installation process and as the system default. Click **Next**.

**Step 13** Select the type of keyboard layout that you want to use. Click **Next**.

**Step 14** Select the **Basic Storage Devices** option. Click **Next**

**Step 15** In the **Hostname** field, type a unique name of your server.  
The host name can include letters, numbers, and hyphens.

**Step 16** Click **Configure Network**.

The Network Connections window is displayed.

**Step 17** Select **System eth0**. Click **Edit**.

**Step 18** Configure the parameters:



#### CAUTION

---

*Configure the Network Connection settings using the same addressing as configured for your pre-upgrade system. If you change any of the settings, your upgrade will fail.*

---

- a Select the **Connect automatically** check box.

- b Click the **IPv4 Settings** tab.

- c From the **Manual** list box, select **Manual**.

- d In the Addresses pane, click **Add**, and then add the IP, Netmask, and Gateway addresses for your server.

- e In the **DNS servers** field, type a comma-separated list of DSN servers.

- f Click **Apply**.

**Step 19** Click **Next** to advance to the next page.

**Step 20** From the list box, select a time zone. Click **Next**.

**Step 21** Configure your root password for your system:

- a In the **Root Password** field, type a root password.

- b In the **Confirm** field, type the root password again.

- c Click **Next** to advance to the next page.

**Step 22** Select the **Create Custom Layout** option. Click **Next**.

**Step 23** Configure disk partitioning:



**CAUTION**

*Do not reformat the following partitions or their sub-partitions: /store, /store/tmp, /store/ariel, /store/ariel/persistent data. If you reformat these partitions, your upgrade will fail.*

- a Configure the mount points for each disk partition.
- b For all other partitions, such as /, /boot, /recovery, configure the file system type to be EXT4.
- c Reformat the swap partition with a file system type of swap

If you want to delete and recreate these partitions instead of editing them, use the following table as a guide:

**Table 1-1** Partitioning

| Partition  | Description                                                               | Mount Point | File System Type | Size                                                                                                                                                                                                                                               | Forced to be primary | SDA or SDB |
|------------|---------------------------------------------------------------------------|-------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|------------|
| /boot      | System boot files                                                         | /boot       | EXT4             | 101 MB                                                                                                                                                                                                                                             | Yes                  | SDA        |
| swap       | Area to be used as memory when RAM is full.                               | empty       | swap             | For systems with 4 to 8 GB of RAM, the size of the swap partition must match the amount of RAM, For systems with 8 to 24 GB of RAM, configure the swap partition size to be 75% of RAM, with a minimum value of 8 GB and a maximum value of 24 GB. | No                   | SDA        |
| /          | Install area for QRadar SIEM, the operating system, and associated files. | /           | EXT4             | Use existing file system size                                                                                                                                                                                                                      | No                   | SDA        |
| /store/tmp | Storage area for QRadar SIEM temporary files                              | /store/tmp  | EXT3             | 20000 MB                                                                                                                                                                                                                                           | No                   | SDA        |
| /var/log   | Storage area for QRadar SIEM and system log files                         | /var/log    | EXT3             | 20000 MB                                                                                                                                                                                                                                           | No                   | SDA        |
| /store     | Storage area for all QRadar SIEM data and configuration files             | /store      | EXT3             | Use existing file system size                                                                                                                                                                                                                      | No                   | SDA        |

**Step 24** Click **Next**.

No changes are required on this page.

**Step 25** Click **Next**.

**Step 26** Select the **Basic Server** option. Click **Next**.

The operating system installation proceeds.

**Step 27** When the installation is complete, click **Reboot**.

**Step 28** Using SSH, log in to QRadar SIEM as the root user.

Username: **root**

Password: **<password>**

**Step 29** Verify that the eth0 interface is configured correctly by typing the following command:

```
ifconfig eth0
```

If interface configuration information is displayed, the eth0 interface is configured correctly.

The eth0 interface is not configured correctly and your upgrade will fail if the following error message is displayed:

```
eth0: error fetching interface information: Device not found
```

If this error message is displayed, contact Customer Support.

**Step 30** Copy the QRadar SIEM 7.1.0 (MR1) ISO file from the location where you downloaded the ISO to the /root/ partition.

**Step 31** Unmount all mounts under the /store partition:

a List the mounts by the typing the following command:

```
mount | grep ' on /store' | cut -d' ' -f3 | sort -r
```

b Unmount all listed mounts in the listed order, using the `umount` command.

For example: `umount /store/tmp`

**Step 32** Mount the /store/tmp folder by typing the following commands:

```
mkdir -p /store/tmp
```

```
mount /store/tmp
```

**Step 33** Create the /media/cdrom folder by typing the following command:

```
mkdir /media/cdrom
```

**Step 34** Mount the QRadar SIEM 7.1.0 (MR1) ISO by typing the following command:

```
mount -o loop <ISO file name> /media/cdrom
```

**Step 35** To run the setup script, type the following command:

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

The End User License Agreement (EULA) is displayed.

**Step 36** Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The following prompt is displayed:

```
About to install version 7.1.0-<build>. Do you wish to continue
(Y/[N])?
```

**Step 37** To continue, type `y`.

After an extended period of time, a message is displayed advising that you are required to restart the system.



### CAUTION

---

*If the upgrade script detects that your system is configured with an off-board storage solution, you are prompted to remount your off-board storage device. For instruction on how to reconfigure off-board storage, see the Reconfiguring Offboard Storage During an Upgrade to QRadar SIEM 7.1.0 (MR1) Technical Note.*

---

**Step 38** Press Enter to select **OK**.

You are prompted to restart your system.

**Step 39** To restart your system, type the following commands:

```
cd
umount /media/cdrom
reboot
```

**Step 40** Using SSH, log in to QRadar SIEM as the root user.

Username: **root**

Password: **<password>**

Your upgrade is complete. The following message is displayed:

```
This server was upgraded to QRadar 7.1.0 Release <build> on
<date>.
```

---

## Clearing the Cache

If you have trouble accessing the QRadar SIEM user interface after you upgrade to QRadar SIEM 7.1.0 (MR1), we recommend that you clear your Java™ cache. Before you clear the cache, ensure you have only one instance of your browser open. If you have multiple versions of your browser open, the cache fails to clear.

### NOTE

---

The Java™ Runtime Environment must be installed on the desktop system you use to view QRadar SIEM. You can download Java version 1.6.0\_u24 at the following website: <http://java.com/>.

---

To clear your cache and access the QRadar SIEM user interface:

**Step 1** Clear your Java cache:

**a** On your desktop, select **Start > Control Panel**.

The Control Panel is displayed.

**b** Double-click the **Java** icon.

The Java Control Panel is displayed.

**NOTE**


---

If you are using Microsoft® Windows 7 as your operating system, the **Java** icon is typically located under the **Programs** pane, depending on how your Control Panel is configured to display features.

---

- c In the **Temporary Internet Files** pane, click **View**.  
The Java Cache Viewer is displayed.
- d Select all QRadar SIEM Deployment Editor entries.
- e Click the **Delete** icon.
- f Click **Close**.
- g Click **OK**.

**Step 2** Open your web browser.

**Step 3** Clear the cache of your web browser:

- a If you are using the Microsoft Internet Explorer 7.0 or 8.0 web browser, select **Tools > Delete Browsing History**.
- b If you are using the Microsoft Internet Explorer 9.0 web browser, click the gear icon in the right corner of the browser window, select **Internet Options > General**, and then click **Delete** in the **Browsing History** pane.
- c If you are using the Mozilla Firefox 3.6.x web browser and above, select **Tools > Clear Recent History > Clear Now**.

**NOTE**


---

If you are using the Mozilla Firefox web browser, you must clear the cache in the Microsoft Internet Explorer and Mozilla Firefox web browsers.

---

**Step 4** Log in to QRadar SIEM:

`https://<IP Address>`

Where **<IP Address>** is the IP address of the QRadar SIEM system. The default values are:

Username: **admin**

Password: **<password>**

Where **<password>** is the password assigned to QRadar SIEM during the installation process.

For more information on accessing and using QRadar SIEM, see the *IBM Security QRadar SIEM Users Guide* or the *IBM Security QRadar SIEM Administration Guide*.



# A

## NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

This section describes some important notices, trademarks, and compliance information.

---

### Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785 U.S.A.*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation  
170 Tracer Lane,  
Waltham MA 02451, USA*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

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

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



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

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



# INDEX

---

## C

clearing the cache 19  
Contacting customer support 2  
conventions 1

---

## D

documentation conventions 1

---

## I

intended audience 1

---

## P

pretesting your system 6

---

## T

technical documentation 1

---

## U

upgrading QRadar SIEM appliances 9  
upgrading QRadar SIEM software running on your own  
hardware 12

