IBM Security QRadar
Version 7.1.0 (MR1)

Installing QRadar 7.1 Using a Bootable USB Flash-Drive Technical Note

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 11.

CONTENTS

1 INSTALLING QRADAR SIEM 7.1 USING A BOOTABLE USB FLASH-DRIVE

Creating a Bootable USB Flash-Drive 4
Using QRadar SIEM to Create a Bootable USB Flash-drive 4
Using a Linux System to Create a Bootable USB Flash-drive 5
Installing QRadar SIEM Using a USB Flash-Drive. 7
Troubleshooting 8

A NOTICES AND TRADEMARKS

Notices 11
Trademarks 13

1 INSTALLING QRADAR SIEM 7.1 USING A BOOTABLE USB FLASH-DRIVE

This technical note provides information on how to install or reinstall IBM Security QRadar SIEM software on the QRadar SIEM appliances using a bootable USB flash-drive. These appliances are shipped pre-installed with QRadar SIEM software. If you need to re-install QRadar SIEM software and your appliance does not have Internet connectivity, you can copy the create USB script to a Linux-based desktop computer or another QRadar SIEM appliance with internet access in your deployment.

Unless otherwise noted, all references to QRadar SIEM refer to QRadar SIEM and IBM Security QRadar Log Manager.

This document includes the following topics:

- **Creating a Bootable USB Flash-Drive**
- **Installing QRadar SIEM Using a USB Flash-Drive**
- **Troubleshooting**

NOTE

This technical note only applies to full installations; it does not apply to upgrades or patches.

Before installing QRadar SIEM using a bootable USB flash-drive, you must have the following items:

- 2 GB (or larger) USB flash-drive
- QRadar SIEM RedHat 64-bit ISO image file

CAUTION

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

Creating a Bootable USB Flash-Drive

If the system you want to install resides in a QRadar SIEM deployment in which other QRadar SIEM systems are available, you can create a bootable USB flash-drive on another QRadar SIEM system. If the system you want to install is a stand-alone device, you can create a bootable USB flash-drive using a Linux-based desktop system.

This section includes the following topics:

- **Using QRadar SIEM to Create a Bootable USB Flash-drive**
- **Using a Linux System to Create a Bootable USB Flash-drive**

Using QRadar SIEM to Create a Bootable USB Flash-drive

To create a bootable USB flash-drive using a QRadar SIEM 7.1 system:

Step 1 Download the QRadar SIEM 7.1 ISO file to your QRadar SIEM system:

a Access the Qmmunity website (https://qmmunity.q1labs.com//).

b Locate the software version you want to download.

For example, the ISO image may resemble the following:

`Rhe664QRadar7_1_0_<build>.iso`

Where, <build> is the software build for the ISO image.

c Save the file.

d Copy the ISO image to a directory on your QRadar SIEM 7.1 system.

For example, /tmp.

Step 2 Using SSH, log in to your QRadar SIEM system as the root user.

Username: **`root`**

Password: **`<password>`**

Step 3 Insert your USB flash-drive into the USB port on your system.

Depending on your system, it might take up to 30 seconds to recognize a USB flash-drive.

Step 4 To identify the USB flash-drive name, type the **`egrep`** command:

```
dmesg | egrep -A15 'usb-storage: device scan complete'
```

The output may resemble the following:

```
[USB Mass Storage support registered.
[root@impreza-secondary ~]# dmesg | egrep -B15 'usb-storage:
device scan complete'
usb-storage: device found at 4
usb-storage: waiting for device to settle before scanning
Vendor: Staples   Model: Relay UFD         Rev: 1.02
Type:   Direct-Access                    ANSI SCSI revision: 02
SCSI device sdc: 7813120 512-byte hdwr sectors (4000 MB)
```

```
sdc: Write Protect is off
sdc: Mode Sense: 03 00 00 00
sdc: assuming drive cache: write through
SCSI device sdc: 7813120 512-byte hdwr sectors (4000 MB)
sdc: Write Protect is off
sdc: Mode Sense: 03 00 00 00
sdc: assuming drive cache: write through
sdc: sdc1
sd 1:0:0:0: Attached scsi removable disk sdc
sd 1:0:0:0: Attached scsi generic sg2 type 0
usb-storage: device scan complete
```

Step 5 Locate and record the USB device name.

In the example output above, the USB flash-drive device name is sdc.

NOTE

Ensure you use the correct device name. In the example output above the device name is sdc. You should not use sdc1 as the device name.

Step 6 Type the following command to mount the ISO image:

`mount -o loop /tmp/Rhe664QRadar7_1_0_<build>.iso /media/cdrom`

Step 7 Type the following command to copy the create_usb_key script from the mounted ISO to the /tmp directory:

`cp /media/cdrom/post/create_usb_key.sh /tmp/`

Step 8 Type the following command to start the USB creation script:

`/tmp/create_usb_key.sh <path> <usb name>`

For example,

`/tmp/create_usb_key.sh /tmp/Rhe664QRadar7_1_0_<build>.iso sdc`

The process of writing the ISO image to your USB flash-drive takes several minutes to complete. When the ISO is loaded onto the USB flash-drive, a confirmation message is displayed.

Step 9 Remove the USB flash-drive from your QRadar SIEM system.

You are now ready to use your USB flash-drive to install QRadar SIEM on your appliance. For information on installing your QRadar SIEM 7.1 bootable USB key, see **Installing QRadar SIEM Using a USB Flash-Drive**.

Using a Linux System to Create a Bootable USB Flash-drive

To create a bootable USB flash-drive using a Linux-based desktop system:

Step 1 Download the QRadar SIEM ISO file to your Linux-based system:

a Access the Qmmunity website (https://qmmunity.q1labs.com//).

b Locate the software version you want to download.

For example, the ISO image may resemble the following:

Rhe664QRadar7_1_0_<build>.iso

Where, <build> is the software build for the ISO image.

c Save the file.

d Copy the ISO image to a directory on your Linux-based system.

For example, /tmp.

Step 2 Log in to your Linux-based system as the root user.

Username: **root**

Password: **<password>**

Step 3 Insert your USB flash-drive into the USB port on your system.

Depending on your system, it might take up to 30 seconds to recognize a USB flash-drive.

Step 4 To identify the USB flash-drive name, type the **egrep** command:

dmesg | egrep -A15 'usb-storage: device scan complete'

The output may resemble the following:

```
[USB Mass Storage support registered.
[root@impreza-secondary ~]# dmesg | egrep -B15 'usb-storage:
device scan complete'
usb-storage: device found at 4
usb-storage: waiting for device to settle before scanning
Vendor: Staples   Model: Relay UFD         Rev: 1.02
Type:   Direct-Access                     ANSI SCSI revision: 02
SCSI device sdc: 7813120 512-byte hdwr sectors (4000 MB)
sdc: Write Protect is off
sdc: Mode Sense: 03 00 00 00
sdc: assuming drive cache: write through
SCSI device sdc: 7813120 512-byte hdwr sectors (4000 MB)
sdc: Write Protect is off
sdc: Mode Sense: 03 00 00 00
sdc: assuming drive cache: write through
sdc: sdc1
sd 1:0:0:0: Attached scsi removable disk sdc
sd 1:0:0:0: Attached scsi generic sg2 type 0
usb-storage: device scan complete
```

Step 5 Locate and record the USB device name.

In the example output above, the USB flash-drive device name is sdc.

NOTE

Ensure you use the correct device name. In the example output above the device name is sdc. You should not use sdc1 as the device name.

Step 6 Update your Linux-based system to include the following packages:

- syslinux
- mtools

The command to run your package manager is different on every Linux system. For example,

- **CentOS** - Type **`yum install syslinux mtools`**
- **Debian or Ubuntu** - Type **`apt-get install syslinux mtools`**

For more information on the specific package manager for your Linux system, see your vendor documentation.

Step 7 Type the following command to mount the ISO image:

`mount -o loop /tmp/Rhe664QRadar7_1_0_<build>.iso /media/cdrom`

Step 8 Type the following command to copy the create_usb_key script from the mounted ISO to the /tmp directory:

`cp /media/cdrom/post/create_usb_key.sh /tmp/`

Step 9 Type the following command to start the USB creation script:

`/tmp/create_usb_key.sh <path> <usb name>`

For example,

`/tmp/create_usb_key.sh /tmp/Rhe664QRadar7_1_0_<build>.iso sdc`

The process of writing the ISO image to your USB flash-drive takes several minutes to complete. When the ISO is loaded onto the USB flash-drive, a confirmation message is displayed.

Step 10 Remove the USB flash-drive from your QRadar SIEM system.

You are now ready to use your USB flash-drive to install QRadar SIEM on your appliance.

Installing QRadar SIEM Using a USB Flash-Drive

Before installing QRadar SIEM using a bootable USB flash-drive, you must first complete the steps in **Creating a Bootable USB Flash-Drive**.

To install QRadar SIEM on your appliance using a bootable USB flash-drive:

Step 1 Insert the bootable USB flash-drive into the USB port of your QRadar SIEM appliance.

Step 2 Restart the appliance.

Step 3 Press the key required to load the boot menu for your appliance.

Step 4 Select USB as the boot option.

The USB flash-drive prepares for the QRadar SIEM installation. It can take up to an hour to start the installation process.

Step 5 When the login prompt is displayed, log in to the system as the root user.

Step 6 Type **SETUP** to begin the installation.

Step 7 Follow the prompts to install QRadar SIEM. The remaining steps are documented in the installation Guide for your software product.

Troubleshooting

If the install hangs or becomes unresponsive during the bootup process, you can follow the steps below to correct the issue.

To correct an unresponsive USB install:

Step 1 Press Ctrl +C to cancel the installation.

If the appliance does not respond to a Ctrl + C, you might be required to restart your appliance.

Step 2 Remove your USB flash-drive and wait 20 seconds.

Step 3 Insert your USB flash-drive in the USB port.

Step 4 Type the following command to verify the USB device name:

```
dmesg | egrep -A15 'usb-storage: device scan complete'
```

The output may resemble the following:

```
[USB Mass Storage support registered.
[root@impreza-secondary ~]# dmesg | egrep -B15 'usb-storage:
device scan complete'
usb-storage: device found at 4
usb-storage: waiting for device to settle before scanning
Vendor: Staples   Model: Relay UFD         Rev: 1.02
Type:   Direct-Access                    ANSI SCSI revision: 02
SCSI device sdc: 7813120 512-byte hdwr sectors (4000 MB)
sdb: Write Protect is off
sdb: Mode Sense: 03 00 00 00
sdb: assuming drive cache: write through
SCSI device sdc: 7813120 512-byte hdwr sectors (4000 MB)
sdb: Write Protect is off
sdb: Mode Sense: 03 00 00 00
sdb: assuming drive cache: write through
sdb: sdb1
sd 1:0:0:0: Attached scsi removable disk sdb
sd 1:0:0:0: Attached scsi generic sg2 type 0
usb-storage: device scan complete
```

Step 5 Choose one of the following options:

- If the device name has not changed, restart your appliance to begin the USB installation.
- If the device name has changed, go to **Step 6**.

Step 6 Locate and record the new USB device name.

In the example output above, the USB flash-drive device name is sdb. The device name might change after reinserting a USB flash-drive.

NOTE Ensure you use the correct device name. In the example output above the device name is sdb. You should not use sdb1 as the device name.

Step 7 Type the following command to start the USB creation script:

`/tmp/create_usb_key.sh <path> <usb name>`

For example,

`/tmp/create_usb_key.sh /tmp/Rhe664QRadar7_1_0_<build>.iso sdb`

The process of writing the ISO image to your USB flash-drive takes several minutes to complete. When the ISO is loaded onto the USB flash-drive, a confirmation message is displayed.

You are now ready to use your USB flash-drive to install QRadar SIEM on your appliance. For more information, see **Installing QRadar SIEM Using a USB Flash-Drive**.

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 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*.

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