IBM Security QRadar Risk Manager
Version 7.1.0 (MR1)

Upgrade IBM Security QRadar Risk Manager Technical Note

Note: Before using this information and the product that it supports, read the information in on “Notices and trademarks” on page 13.

CONTENTS

1 UPGRADE IBM SECURITY QRADAR RISK MANAGER

Upgrading an IBM Security QRadar Risk Manager appliance from QRadar Risk Manager 1.1 Maintenance Release 5 to QRadar Risk Manager 7.1.0 is a significant update.

Due to the extent of the changes, the upgrade process requires that you backup your existing QRadar Risk Manager 1.1, complete a fresh install of QRadar Risk Manager 7.1.0, and restore your data. No QRadar Risk Manager data is lost during the upgrade process.

Before you begin

Before you upgrade from QRadar Risk Manager Maintenance Release 5 to QRadar Risk Manager 7.1.0, review all of the following information:

- Upgrade requirements
- Impact of an upgrade on your data

Upgrade requirements

Before you begin the upgrade, you must verify the following requirements:

- Your QRadar SIEM Console must be upgraded from QRadar SIEM 7.0 Maintenance Release 5 (7.0.0.301503) to QRadar SIEM 7.1.0. For more information, see the *IBM Security QRadar SIEM Upgrade Guide*.
- To upgrade to QRadar Risk Manager 7.1.0, you must be running QRadar Risk Manager 1.1 Maintenance Release 5 build 312057. If you are not running at least QRadar Risk Manager 1.1 Maintenance Release 5 build 312057, download and install the latest patch update from the Qmmunity website. This version is required to backup your QRadar Risk Manager data.

  In the QRadar SIEM user interface, click **Help > About** to view your QRadar Risk Manager version information. The QRadar Risk Manager version is displayed in the Installed Plug-ins list.
- You must verify that some form of storage is available for the QRadar Risk Manager 1.1 backup file. The backup file must be copied off of the QRadar Risk Manager system for the duration of the upgrade to prevent you from losing your device configurations and data. The restore file contains all of the information from your QRadar Risk Manager 1.1 system. Due to the size and number of devices managed by QRadar Risk Manager, the size of the backup file can vary.

NOTE

Ensure that your QRadar SIEM Console and QRadar Risk Manager use the same network switch.

Impact of an upgrade on your data

All data required to restore your data after upgrading from QRadar Risk Manager 1.1 to QRadar Risk Manager 7.1.0 is contained in a backup archive you create. After the installation of QRadar Risk Manager 7.1.0 completes, you can restore your QRadar Risk Manager settings and data from the backup archive.

The backup archive includes the following data:

- device configurations for QRadar Risk Manager
- connection data
- topology data
- policy monitor questions
- simulation data
- database tables for QRadar Risk Manager

Identifying network settings

Before you upgrade to QRadar Risk Manager 7.1.0, gather the following information:

- QRadar Risk Manager activation key
- hostname
- IP address
- network mask address
- subnet mask
- default gateway address
- primary Domain Name System (DNS) server address
- secondary DNS server (optional) address
- public IP address for networks using Network Address Translation (NAT)
- email server name
- Network Time Protocol (NTP) server (Console only) or time server name

You are now ready to backup the data from your QRadar Risk Manager 1.1 appliance.

Backing up your data

The QRadar Risk Manager backup script must be downloaded from Qmmunity. This script is intended for upgrading QRadar Risk Manager 1.1 to QRadar Risk Manager 7.1.0 or backing up and restoring QRadar Risk Manager 7.1.0 systems.

To create a QRadar Risk Manager backup:

Step 1 Download the QRadar Risk Manager backup script from Qmmunity.

`risk_manager_backup.sh`

Step 2 Copy the backup script to the /tmp directory of your QRadar SIEM Console.

Step 3 Using SSH, log in your QRadar Console as the root user:

Username: **`root`**

Password: **`<password>`**

Step 4 Type the following command to copy the backup script to QRadar Risk Manager:

`scp /tmp/risk_manager_backup.sh root@<QRadar Risk Manager>:/opt/qradar/bin/dbmaint/risk_manager_backup.sh`

Step 5 Type the root password of QRadar Risk Manager to copy the file.

The file is copied from the /tmp directory of your QRadar SIEM Console to the /opt/qradar/bin/dbmaint directory of QRadar Risk Manager.

Step 6 Using SSH from the QRadar SIEM Console, log in to QRadar Risk Manager:

Username: **`root`**

Password: **`<password>`**

Step 7 To start a QRadar Risk Manager backup, type the following command:

`/opt/qradar/bin/dbmaint/risk_manager_backup.sh`

It can take several minutes for the script to start the backup process. After the script completes, the following message is displayed:

```
Tue Sep 11 10:14:41 EDT 2012 - Risk Manager Backup complete,
wrote /store/qrm_backups/backup-2012-09-11-10-14-39.tgz
```

NOTE

By default, QRadar Risk Manager backups are stored in **`/store/qrm_backups/`**.

All backup files are saved using the following format:

`backup-<target date>-<timestamp>.tgz`

Where:

`<target date>` is the date that the backup file was created. The format of the target date is **`<day>_<month>_<year>`**.

`<timestamp>` is the time that the backup file was created. The format of the timestamp is **`<hour>_<minute>_<second>`**.

Step 8 Copy the backup file to a safe location for the upgrade.

CAUTION

The backup file must be stored in a location other than your QRadar Risk Manager appliance. During the upgrade process to QRadar Risk Manager 7.1.0, the disks are partitioned and all existing data is removed. The backup file allows

you to recover all of your settings, data, and configuration information after the upgrade to QRadar Risk Manager 7.1.0 is complete.

You can now install QRadar Risk Manager 7.1.0.

Installing QRadar Risk Manager

To install to QRadar Risk Manager:

Step 1 Log in to the Qmmunity and download the QRadar ISO.

Previously, QRadar Risk Manager and QRadar used unique ISO images for installations. In the 7.1.0 release, QRadar Risk Manager and QRadar are merged and both products are installed using the QRadar ISO file. The activation key specified during the installation determines which product is installed.

Step 2 Copy the QRadar SIEM 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*.

Step 3 Insert the portable storage device into your appliance.

Step 4 Restart your QRadar Risk Manager appliance.

Step 5 To load the boot menu, press the F11 or the Escape key on your keyboard.

Step 6 Select USB drive or DVD drive as the boot option.

NOTE

QRadar Risk Manager verifies the integrity of the media before installation by checking the MD5 sum. If you receive a warning message that the MD5 checksum failed, then you are required to re-download or re-burn QRadar Risk Manager. For further assistance, contact Customer Support.

Step 7 Type **SETUP** to start the installation.

Step 8 When the localhost login prompt is displayed, type **root** to log in to the system.

The End User License Agreement (EULA) is displayed.

Step 9 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 activation key window is displayed. The activation key is a 24-digit, four-part, alphanumeric string.

You can find the activation key:

- Printed on a sticker and physically placed on your appliance.
- Included with the packing slip; all appliances are listed along with their associated keys.

Step 10 Type your activation key and press Enter.

NOTE

The letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

Step 11 Select **normal** for your type of setup. Select **Next**.

Step 12 Select your time zone continent or area. Select **Next** and press Enter.

Step 13 Select your time zone region. Select **Next** and press Enter.

Step 14 Select an internet protocol version. Select **Next** and press Enter.

Step 15 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

The window displays up to a maximum of four interfaces depending on your hardware configuration. Each interface with a physical link is denoted with a plus (+) symbol.

Step 16 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to**Step 19**.
- If you are using IPv6 as your Internet protocol, go to**Step 17**.

Step 17 Choose one of the following options:

a To automatically configure for IPv6, select **Yes** and press Enter. The automatic configuration can take an extended period of time. Go to**Step 19**.

b To manually configure for IPv6, select **No** and press Enter. Go to**Step 18**.

Step 18 To enter network information to use for IPv6:

a In the **Hostname** field, type a fully qualified domain name as the system hostname.

b In the **IP Address** field, type the IP address of the system.

c In the **Email server** field, type the email server. If you do not have an email server, type `localhost` in this field.

d Select **Next** and press Enter. Go to**Step 20**.

Step 19 Configure the QRadar Risk Manager IPv4 network settings:

a Enter values for the following parameters:

- **Hostname** - Type a fully qualified domain name as the system hostname.
- **IP Address** - Type the IP address of the system.
- **Network Mask** - Type the network mask address for the system.
- **Gateway** - Type the default gateway of the system.
- **Primary DNS** - Type the primary DNS server address.
- **Secondary DNS** - Optional. Type the secondary DNS server address.
- **Public IP** - Optional. Type the Public IP address of the server. This is a secondary IP address that is used to access the server, usually from a

different network or the Internet, and is managed by your network administrator. The Public IP address is often configured 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** - Type the email server. If you do not have an email server, type **`localhost`** in this field.

b Select **Next** and press Enter.

Step 20 Configure the QRadar Risk Manager root password:

a Type your password. Select **Next** and press Enter

b Retype your new password to confirm. Select **Finish** and press Enter.

A series of messages are displayed as QRadar Risk Manager continues with the installation. This process typically takes several minutes.

Step 21 Press Enter to select **OK**.

You are now ready to restore your data to QRadar Risk Manager.

Restoring Your Data

QRadar Risk Manager uses a separate script for restoring data, which allows you to restore data from a QRadar Risk Manager backup. The restore script allows you to specify the archive you are restoring to QRadar Risk Manager. This process requires you to stop services on QRadar Risk Manager, which logs off all QRadar Risk Manager users and stops multiple processes.

NOTE

The QRadar Risk Manager appliance and the backup archive must be from an identical version of QRadar Risk Manager. If the script detects a version difference between the archive and the QRadar Risk Manager managed host, an error is displayed.

To restore a QRadar Risk Manager from a backup archive:

Step 1 Using SSH, log in your QRadar Risk Manager as the root user:

Username: **`root`**

Password: **`<password>`**

Step 2 Type the following command to stop hostcontext:

```
service hostcontext stop
```

Step 3 To restore a backup archive to QRadar Risk Manager, type the following command:

```
/opt/qradar/bin/risk_manager_restore.sh -r
/store/qrm_backups/<backup>
```

Where **`<backup>`** is the QRadar Risk Manager archive you want to restore.

For example:

```
/opt/qradar/bin/risk_manager_restore.sh -r
/store/qrm_backups/backup-2012-09-11-10-14-39.tgz
```

Table 1 Optional restore parameters

Parameters	Description
-f	Overwrites any existing QRadar Risk Manager data on your system with the data in the restore file. Selecting this parameter
-w	Do not delete directories before restoring QRadar Risk Manager data.
-h	Displays the help for the restore script.

The following message is displayed:

```
Tue Sep 11 16:47:22 EDT 2012 - Risk Manager Restore v1 - starting
risk_manager_restore.sh; ArchiveFile=/store/qrm_backups/backup-201
12-09-11-16-27-42.tgz, Force Overwrite=true
Tue Sep 11 16:47:22 EDT 2012 - Risk Manager Restore v1 - Appliance is QRM
Tue Sep 11 16:47:22 EDT 2012 - Risk Manager Restore v1 - archive is from version
'372011'
Tue Sep 11 16:47:23 EDT 2012 - Risk Manager Restore v1 - appliance version is 372011
Tue Sep 11 16:47:33 EDT 2012 - Risk Manager Restore v1 - restoring db postgres
Tue Sep 11 16:47:34 EDT 2012 - Risk Manager Restore v1 - restoring db qradar
Tue Sep 11 16:47:36 EDT 2012 - Risk Manager Restore v1 - restoring db ziptie
Tue Sep 11 16:47:36 EDT 2012 - Risk Manager Restore v1 - complete.
```

QRadar Risk Manager data is restored from the backup archive.

Step 4 Type the following command to start hostcontext:

```
service hostcontext start
```

After the hostcontext services are started, then the data restore from the backup archive is complete.

You are now ready to add QRadar Risk Manager as a managed host in QRadar.

Adding QRadar Risk Manager to QRadar SIEM

To add QRadar Risk Manager as a managed host to your QRadar SIEM Console:

Step 1 Open your web browser.

Step 2 Log in to your QRadar SIEM Console:

`https://<IP Address>`

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

Username: **`admin`**

Password: **`<root password>`**

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

Step 3 On the **Admin** tab, click **Deployment Editor**.

The Event View page is displayed.

Step 4 From the menu, select **Actions > Add a Managed Host**.

The Add New Managed Host wizard is displayed.

Step 5 Click **Next**.

The Enter the Host's IP page is displayed.

Step 6 Enter values for the parameters:

- **Enter the IP of the server or appliance to add** - Type the IP address of QRadar Risk Manager.
- **Enter the root password of the host** - Type the root password for the host.
- **Confirm the root password of the host** - Type the password again.
- **Host is NATed** - Select the check box to use an existing Network Address Translation (NAT) on this managed host. For more information on NAT, see the *IBM Security QRadar SIEM Administration Guide*.

NOTE

If you want to enable NAT for a managed host, the NATed network must be using static NAT translation. For more information, see the *IBM Security QRadar SIEM Administration Guide.*

- **Enable Encryption** - Select the check box to create an SSH encryption tunnel for the host. To enable encryption between two managed hosts, each managed host must be running QRadar 7.1.0 or QRadar Risk Manager 7.1.0.
- **Enable Compression** - Select the check box to enable data compression between two managed hosts, each managed host must be running at least QRadar 7.1.0 or QRadar Risk Manager 7.1.0.

If you selected the Host is NATed check box, the Configure NAT Settings page is displayed. Go to**Step 7**. Otherwise, go to**Step 8**.

NOTE

If you want to add a non-NATed managed host to your deployment when the Console is NATed, you must change the Console to a NATed host before adding the managed host to your deployment. For more information, see the *IBM Security QRadar SIEM Administration Guide.*

Step 7 To select a NATed network, enter values for the following parameters:

- **Enter public IP of the server or appliance to add** - Type the public IP address of the managed host. The managed host uses this IP address to communicate with other managed hosts in different networks using NAT.
- **Select NATed network** - From the list box, select the network you want this managed host to use.

- If the managed host is on the same subnet as the Console, select the Console of the NATed network.
- If the managed host is not on the same subnet as the Console, select the managed host of the NATed network.

NOTE

For information on managing your NATed networks, see the *IBM Security QRadar SIEM Administration Guide*.

Step 8 Click **Next**.

Step 9 Click **Finish**.

NOTE

This process can take several minutes to complete. If your deployment included undeployed changes, a window is displayed requesting you to deploy all changes.

Step 10 Click **Deploy**.

The System View is displayed, including the host in the Managed Hosts pane. You are now ready to clear your cache. The **Risks** tab is not visible until you clear your browser cache and log in to QRadar SIEM.

Clearing web browser 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 can fail to clear properly.

To clear your web browser cache:

Step 1 Open your web browser.

Step 2 Clear the cache of your web browser:

a If you are using Internet Explorer 8.0, select **Tools > Delete Browsing History > Delete**.

b If you are using Internet Explorer 9.0, click the gear icon in right corner of the browser window, select **Internet Options > General**, and then click **Delete** in the **Browsing History** section.

c If you are using Mozilla Firefox, select **Tools > Options > Advanced > Network > Clear Now**.

NOTE

If you are using a Mozilla Firefox web browser, you must clear the cache in the Microsoft Internet Explorer web browser as well.

Step 3 Log in to QRadar SIEM.

A NOTICES AND TRADEMARKS

What's in this appendix:

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

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