IBM Security QRadar Risk Manager
Version 7.1.0 (MR1)

Installation Guide

Note: Before using this information and the product that it supports, read the information in “Notices and trademarks”on page page 23.

CONTENTS

ABOUT THIS GUIDE

The *IBM Security QRadar Risk Manager Installation Guide* provides you with information on setting up QRadar Risk Manager. QRadar Risk Manager appliances are pre-installed with software and a Red Hat Enterprise Linux operating system; however, you can install QRadar Risk Manager software on your own hardware. This guide assumes a working knowledge of networking and Linux systems.

Intended audience

This guide is intended for network administrators responsible to installing and configuring QRadar Risk Manager systems in your network.

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 Documentation Technical Note***. (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 PREPARE FOR YOUR INSTALLATION

Your IBM Security QRadar Risk Manager deployment can consist of a IBM Security QRadar Risk Managerappliance installed as a managed host on your IBM Security QRadar SIEM Console. Only one QRadar Risk Manager is allowed on a QRadar SIEM Console in your deployment.

Before you install

You must complete the installation process for a IBM Security QRadar SIEM Console before you install IBM Security QRadar Risk Manager. You should install QRadar SIEM and QRadar Risk Manager on the same network switch.

For information about installing QRadar SIEM, including additional hardware and software requirements, see *IBM Security QRadar SIEM Installation Guide*.

As of version 7.1 of QRadar Risk Manager, QRadar SIEM and QRadar Risk Manager share the same installation ISO and installation process. This allows you to add QRadar Risk Manager to your deployment using the deployment editor in QRadar SIEM.

A QRadar Risk Manager appliance installation includes the QRadar Risk Manager software and a Red Hat Enterprise Linux operating system.

Since IBM Security QRadar Risk Manager is a 64-bit appliance, make sure that you download the correct installation software for your operating system.

Identify network settings

Before you install QRadar Risk Manager, gather the following information:

- 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

Port requirements

Ensure that any firewall that is located between the QRadar SIEM Console and QRadar Risk Manager allows traffic on the following ports:

- Port 443 (HTTPS)
- Port 22 (SSH)
- Port 37 UDP (Time)

Unsupported features

QRadar Risk Manager does not support the following features:

- High Availability (HA)
- Dynamic Routing
  - Border Gateway Protocol (BGP)
  - Open Shortest Path First (OSPF)
  - Routing Information Protocol (RIP)
- IPv6
- Non-contiguous Network Masks

Additional hardware requirements

Before you install IBM Security QRadar Risk Manager systems, you need access to the following additional hardware components:

- Monitor and keyboard or a serial console
- Uninterrupted Power Supply (UPS)

NOTE

To ensure that your QRadar Risk Manager data is preserved during a power failure, equip all QRadar Risk Manager appliances or systems running QRadar Risk Manager software that store data, such as Consoles, Event Processors, or QFlow Collectors with an Uninterrupted Power Supply (UPS).

Additional software requirements

The following software must be installed on the desktop system that you use to access the QRadar Risk Manager user interface:

- Java™ Runtime Environment
- Adobe Flash, version 10 or higher

Supported web browsers

You can access the Console from a standard web browser. When you access the system, a prompt is displayed asking for a user name and a password, which must be configured in advance by the QRadar Risk Manager administrator.

Table 1-1 Supported Web Browsers

Web Browser	Supported Versions
Mozilla Firefox	• 10.0 Due to Mozilla's short release cycle, we cannot commit to testing on the latest versions of the Mozilla Firefox browser. However, we are fully committed to investigating any issues that are reported.
Microsoft Internet Explorer, with Compatibility View Enabled	• 8.0 • 9.0 For instructions on how to enable Compatibility View, see Enabling Compatibility View for Microsoft Internet Explorer.

Enabling Compatibility View for Microsoft Internet Explorer

To enable Compatibility View for Microsoft Internet Explorer 8.0 and 9.0:

Step 1 Press F12 to open the Developer Tools window.

Step 2 Configure the following compatibility settings:

Table 1-2 Microsoft Internet Explorer Compatibility Settings

Browser Version	Option	Description
Microsoft Internet Explorer 8.0	Browser Mode	From the **Browser Mode** list box, select **Internet Explorer 8.0.**
	Document Mode	From the **Document Mode** list box, select **Internet Explorer 7.0 Standards.**
Microsoft Internet Explorer 9.0	Browser Mode	From the **Browser Mode** list box, select **Internet Explorer 9.0.**
	Document Mode	From the **Document Mode** list box, select **Internet Explorer 7.0 Standards.**

Use the installation wizard

The following table provides information about the install wizard navigation.

Table 1-3 Installation Wizard Actions

If you want to	Perform this action
Move to another option on a page	Press the Up or Down arrows to move the cursor through configurable options on the installation wizard page.
Select an option from a list	Press the Spacebar to select your chosen option on a list. When you select an option, an X is displayed in the parentheses next to the option.
Select a navigation option	Press Tab to move the cursor from the configurable options to the **Next**, **Back**, and **Finish** options.
Select a navigation option	Press Enter on the keyboard.

Accessing the QRadar Risk Manager user interface

After the installation is complete, you can access QRadar Risk Manager from the **Risks** tab in the QRadar SIEM user interface.

To access the QRadar SIEM user interface:

Step 1 Open your web browser.

Step 2 Log in to QRadar SIEM:

`https://<IP Address>`

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

Username: `admin`

Password: `<root password>`

Where `<root password>` is the password assigned to QRadar Risk Manager during the installation process.

NOTE

If you are using a Mozilla Firefox web browser then you must add an exception to Mozilla Firefox to log in to QRadar SIEM. For more information, see your Mozilla documentation. If you are using a Microsoft Internet Explorer web browser, a website security certificate message is displayed. You must select the Continue to this website option to log in to QRadar SIEM.

Step 3 Click **Login To QRadar**.

For your QRadar SIEM Console and QRadar Risk Manager managed host, a default license key provides you access to the system for five weeks. For more information on the license key, see the *IBM Security QRadar SIEM Administration Guide*.

2 INSTALL IBM SECURITY QRADAR RISK MANAGER APPLIANCES

An IBM Security QRadar Risk Manager deployment includes a IBM Security QRadar SIEM Console and QRadar Risk Manager appliance as a managed host.

Before you begin

You need to prepare your appliance before you install a IBM Security QRadar Risk Manager appliance.

Before you begin you need to install all necessary hardware. For information on your QRadar Risk Manager appliance, see the *IBM QRadar Hardware Installation Guide*.

You need an activation key before you install QRadar Risk Manager. If you do not have an activation key with your QRadar Risk Manager appliance, contact support at: *welcomecenter@q1labs.com*.

To prepare to install a QRadar Risk Manager appliance:

Step 1 Choose one of the following options:

- Connect a laptop to the serial port on the rear of the appliance.

  If you use a laptop to connect to the system, you must use a terminal program, such as HyperTerminal, to connect to the system. Make sure you set **Connect Using** to the appropriate COM port of the serial connector and **Bits per second** to 9600. You must also set **Stop Bits** (1), **Data bits** (8), and **Parity** (None).

- Connect a keyboard and monitor to their respective ports.

  For more information on appliance ports, see the *Hardware Installation Guide*.

Step 2 Power on the system and log in:

Username: `root`

The username is case sensitive.

Step 3 Press Enter.

Step 4 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document.

Step 5 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 that you receive from Q1 Labs.

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 6 Type your activation key and press Enter.

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

Installing QRadar Risk Manager

You must complete the preparation steps before you can install IBM Security QRadar Risk Manager.

To install QRadar Risk Manager:

Step 1 Select **normal** for the type of setup. Select **Next** and press Enter.

Step 2 Select your time zone continent or area. Select **Next** and press Enter.

Step 3 Select your time zone region. Select **Next** and press Enter.

Step 4 Select an internet protocol version. Select **Next** and press Enter.

Step 5 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 6 Choose one of the following options:

- If you are using IPv6 as your Internet protocol, go to**Step 7**.
- If you are using IPv4 as your Internet protocol, go to **Step 9**.

Step 7 To automatically configure for IPv6, select **Yes** and press Enter. The automatic configuration can take an extended period of time. Go to **Step 9**. To manually configure for IPv6, select **No** and press Enter. Go to **Step 8**.

Step 8 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 10**.

Step 9 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 10 To configure the QRadar Risk Manager root password, type your password.

Step 11 Select **Next** and press Enter

Step 12 Retype your new password to confirm. Select **Finish** and press Enter.

This process typically takes several minutes.

Step 13 Press Enter to select **OK**.

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

Step 14 Press Enter to select **OK**.

You are now ready to add QRadar Risk Manager as a managed host to your QRadar SIEM Console.

Adding QRadar Risk Manager to QRadar SIEM

To add IBM Security 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 SIEM during the installation process.

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

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

Step 5 Click **Next**.

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. 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 SIEM 7.1 or QRadar Risk Manager 7.1.
- **Enable Compression** - Select the check box to enable data compression between two managed hosts. Each managed host must be running at least QRadar SIEM 7.1 or QRadar Risk Manager 7.1.

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.

Step 8 Click **Next**.

Step 9 Click **Finish**.

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 **Risks** tab appears after you clear your browser cache and log in to QRadar SIEM.

Clearing the web browser cache

You must clear the browser cache before you can access the **Risks** tab in QRadar SIEM.

Ensure that you only have one web browser open. If you have multiple browsers open, the cache can fail to clear properly.

To clear the web browser cache:

Step 1 Open your web browser.

Step 2 Clear the cache of your web browser:

- **a** If you are using Microsoft Internet Explorer 8.0, select **Tools > Delete Browsing History > Delete**.
- **b** If you are using Microsoft 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 Microsoft Internet Explorer as well.

Defining user roles

Before you can allow access to IBM Security QRadar Risk Manager functionality to other users in your organization, you must assign the appropriate user role permissions. By default, QRadar SIEM provides a default administrative role, which provides access to all areas of QRadar Risk Manager. Any QRadar SIEM user that requires access to the Risks tab needs to have the Risk Manager user role.

For information about creating and managing user roles, see the *IBM Security QRadar SIEM Administration Guide*.

To assign a QRadar Risk Manager user role permissions:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 In the **User Management** pane, click the **User Roles** icon.

Step 4 Click the **Edit** icon next to the user role you want to edit.

Step 5 Select the **Risk Manager** check box.

Step 6 Click **Next**.

If you added Risk Manager to a user role that has Log Activity permission, then you need to define the log sources the user role can access. You can add an entire log source group by clicking the **Add** icon in the Log Source Group pane. You can

select multiple log sources by holding the Control key while you select each log source you want to add.

Step 7 Click **Return**.

Step 8 From the **Admin** tab menu, click **Deploy Changes**.

Troubleshoot the Risks tab

If the **Risks** tab does not display properly or is inaccessible, then you need to remove and then re-add IBM Security QRadar Risk Manager as a managed host on your QRadar SIEM Console.

Removing QRadar Risk Manager as a managed host

To remove a QRadar Risk Manager managed host from your deployment, you must:

Step 1 Log in to QRadar SIEM:

`https://<IP Address>`

Where **`<IP Address>`** is the IP address of the QRadar SIEM Console.

Username: **`admin`**

Password: **`<admin password>`**

Step 2 Click the **Admin** tab.

Step 3 Click the **Deployment Editor** icon.

Step 4 Click the **System View** tab.

Step 5 Right-click the managed host that you want to delete and select **Remove host**.

Repeat for each non-Console managed host until all hosts are deleted.

Step 6 Click **Save**.

Step 7 Close the deployment editor.

Step 8 On the **Admin** tab, click **Deploy Changes**.

Re-Adding QRadar Risk Manager as a managed host

To re-add IBM Security QRadar Risk Manager as a managed host, you must:

Step 1 Log in to QRadar SIEM:

`https://<IP Address>`

Where **`<IP Address>`** is the IP address of the QRadar SIEM Console.

Username: **`admin`**

Password: **`<admin password>`**

Step 2 Click the **Admin** tab.

Step 3 Click the **Deployment Edit** icon.

The deployment editor is displayed.

Step 4 Click the **System View** tab.

Step 5 From the menu, select **Actions > Add a managed host**.

Step 6 Click **Next**.

Step 7 Enter values for the parameters:

- **Enter the IP of the QRadar Risk Manager appliance** - Type the IP address of your QRadar Risk Manager appliance.
- **Enter the root password of the host** - Type the root password for QRadar Risk Manager.
- **Confirm the root password of the host** - Type the password again, for confirmation.
- **Host is NATed** - Select this option if you want to specify NAT values if necessary.
- **Enable Encryption** - Select this option if you want to enable encryption.

Step 8 Click **Next**.

Step 9 Click **Finish**.

The process of adding QRadar Risk Manager can take several minutes to complete.

Step 10 Close the deployment editor.

Step 11 On the **Admin** tab, click **Deploy Changes**.

The changes are deployed. If you are still experiencing issues viewing the **Risks** tab on QRadar SIEM, contact customer support.

3 CHANGE NETWORK SETTINGS

To change the network settings of a IBM Security QRadar Risk Manager appliance attached to a IBM Security QRadar SIEM Console, you must remove QRadar Risk Manager as a managed host in the deployment, change the network settings, and re-add the managed host.

You must perform this procedure in the following order:

1. Removing QRadar Risk Manager as a managed host
2. Changing the network settings
3. Re-Adding QRadar Risk Manager as a managed host

NOTE This procedure requires you to use the deployment editor. For more information on using the deployment editor, see the *IBM Security QRadar SIEM Administration Guide*.

Removing QRadar Risk Manager as a managed host

To remove a QRadar Risk Manager managed host from your deployment, you must:

Step 1 Log in to QRadar SIEM:

`https://<IP Address>`

Where `<IP Address>` is the IP address of the QRadar SIEM Console.

Username: `admin`

Password: `<admin password>`

Step 2 Click the **Admin** tab.

Step 3 Click the **Deployment Editor** icon.

Step 4 Click the **System View** tab.

Step 5 Right-click the managed host that you want to delete and select **Remove host**.

Repeat for each non-Console managed host until all hosts are deleted.

Step 6 Click **Save**.

Step 7 Close the deployment editor.

Step 8 On the Admin tab, click **Deploy Changes**.

Changing the network settings

To change the network settings, you must:

Step 1 Using SSH, log in to QRadar Risk Manager as the root user.

Username: **root**

Password: **<password>**

Step 2 Type the following command:

qchange_netsetup

Step 3 Select an internet protocol version. 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 4 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 5 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to Step 8.
- If you are using IPv6 as your Internet protocol, go to Step 6.

Step 6 To configure IPv6, 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 8.

b To manually configure for IPv6, select **No** and press Enter. Go to Step 7.

Step 7 To enter network information to use for IPv6:

a Type the values for the **Hostname**, **IP Address**, and **Email server**.

b Select **Next** and press Enter.

Step 8 Configure the QRadar Risk Manager 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 name of the email server. If you do not have an email server, type **localhost** in this field.

b Select **Next** and press Enter.

Step 9 Select **Finish** and press Enter.

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

Re-Adding QRadar Risk Manager as a managed host

To re-add QRadar Risk Manager as a managed host, you must:

Step 1 Log in to QRadar SIEM:

https://<IP Address>

Where **<IP Address>** is the IP address of the QRadar SIEM Console.

Username: **admin**

Password: **<admin password>**

Step 2 Click the **Admin** tab.

Step 3 Click the **Deployment Edit** icon.

Step 4 Click the **System View** tab.

Step 5 From the menu, select **Actions > Add a managed host**.

Step 6 Click **Next**.

Step 7 Enter values for the parameters:

- **Enter the IP of the QRadar Risk Manager appliance** - Type the IP address of your QRadar Risk Manager appliance.
- **Enter the root password of the host** - Type the root password for QRadar Risk Manager.
- **Confirm the root password of the host** - Type the password again, for confirmation.
- **Host is NATed** - Select this option if you want to specify NAT values if necessary.
- **Enable Encryption** - Select this option if you want to enable encryption.

Step 8 Click **Next**.

Step 9 Click **Finish**.

The process of adding QRadar Risk Manager can take several minutes to complete.

Step 10 Close the deployment editor.

Step 11 Click **Deploy Changes**.

4 RE-INSTALL IBM SECURITY QRADAR RISK MANAGER FROM THE RECOVERY PARTITION

You might need to re-install your software from the recovery partition. When you re-install IBM Security QRadar Risk Manager from the IBM Security QRadar SIEM ISO on the recovery partition, your system is restored back to factory default configuration, meaning that your current configuration and data files are overwritten. Before you begin, review the guidelines for navigating the installation wizard. See Use the installation wizard.

This information applies to new QRadar Risk Manager installations or upgrades from new QRadar Risk Manager installations on QRadar Risk Manager appliances.

When you install QRadar Risk Manager, the installer (QRadar SIEM ISO) is copied into the recovery partition. From this partition, you can re-install QRadar Risk Manager, which restores QRadar Risk Manager to factory defaults.

NOTE

Any software upgrades that you perform after you install QRadar Risk Manager replaces the ISO file with the newer version.

When you reboot your QRadar Risk Manager appliance, you are presented with the option to re-install the software. Since QRadar SIEM and QRadar Risk Manager share the same ISO installation file, the name display shows the QRadar SIEM ISO name. If you do not respond to the prompt after 5 seconds, the system reboots as normal, thus maintaining your configuration and data files. If you choose the re-install QRadar SIEM ISO option, a warning message is displayed and you must confirm that you want to re-install the software. After confirmation, the installer runs and you can follow the prompts through the installation process.

After a hard disk failure, you are unable to re-install from the recovery partition, because it is longer be available. If you experience a hard disk failure, contact Customer Support for assistance.

Preparing for Re-installation from a Recovery Partition

You need to prepare for the re-installation before you can re-add IBM Security QRadar Risk Manager as a manage host.

Before you begin, ensure that you have your activation key, which i s a 24-digit, four-part, alphanumeric string that you receive from Q1 Labs.

You can find the key:

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

If you do not have your activation key, contact the Welcome Center at welcomecenter@q1labs.com with the serial number of the QRadar Risk Manager appliance. Software activation keys do not require serial numbers.

To prepare for re-installation:

Step 1 Reboot your QRadar Risk Manager appliance.

Step 2 Select **Factory re-install**.

Step 3 Type **`flatten`** to continue.

The installer partitions and reformats the hard disk, installs the OS, and then re-installs QRadar Risk Manager. You must wait for the flatten process to complete. This process can take up to several minutes, depending on your system.

Step 4 Type **`SETUP`**.

Step 5 Log in to QRadar Risk Manager as the root user.

Step 6 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.

Step 7 Type your activation key and press Enter. The letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

Step 8 Select **normal** for the type of setup. Select **Next** and press Enter.

Step 9 Select your time zone continent or area. Select **Next** and press Enter.

Step 10 Select your time zone region. Select **Next** and press Enter.

Step 11 Select an internet protocol version. Select **Next** and press Enter.

Step 12 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 13 Choose one of the following options:

- If you are using IPv6 as your Internet protocol, go to Step 14.
- If you are using IPv4 as your Internet protocol, go to Step 16.

Step 14 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 16.

b To manually configure for IPv6, select **No** and press Enter. Go to Step 15.

Step 15 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 17.

Step 16 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 17 Configure the QRadar Risk Manager root password:

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

The Confirm New Root Password window is displayed.

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

This process typically takes several minutes.

The Configuration is Complete window is displayed.

Step 18 Press Enter to select **OK**.

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

Step 19 Press Enter to select **OK**.

You are now ready to add QRadar Risk Manager as a managed host to your QRadar SIEM Console. For more information, see Adding QRadar Risk Manager 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*.

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.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

INDEX