

IBM Security QRadar Risk Manager  
Version 7.2.1

*Installation Guide*



**Note**

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

---

# Contents

<b>Introduction to installing IBM Security QRadar Risk Manager.</b>	<b>v</b>
<b>Chapter 1. Prepare to install IBM Security QRadar Risk Manager</b>	<b>1</b>
Before you install.	1
Identify network settings	1
Configure port access on firewalls	1
Unsupported features in QRadar Risk Manager.	2
Additional hardware requirements	2
Additional software requirements	2
Supported web browsers	2
Enabling document mode and browser mode in Internet Explorer	3
<b>Chapter 2. Install IBM Security QRadar Risk Manager appliances</b>	<b>5</b>
Preparing your appliance	5
Access the IBM Security QRadar Risk Manager user interface	6
Network parameter information for IPv4	6
Installing IBM Security QRadar Risk Manager	7
Adding QRadar Risk Manager to QRadar SIEM	7
Clearing web browser cache	9
Risk Manager user role	9
Assigning the Risk Manager user role	9
Troubleshoot the Risks tab	10
Removing a managed host	10
Readd QRadar Risk Manager as a managed host.	10
<b>Chapter 3. Reinstall QRadar from the recovery partition</b>	<b>13</b>
Reinstalling QRadar Risk Manager by using Factory re-install	13
<b>Chapter 4. Change network settings</b>	<b>15</b>
Removing a managed host	15
Change network settings	15
Readd QRadar Risk Manager as a managed host.	16
<b>Chapter 5. Data back up and restore</b>	<b>19</b>
Prerequisites for backing up and restoring data	19
Backing up your data	20
Restoring data	20
<b>Notices</b>	<b>23</b>
Trademarks	24
Privacy policy considerations	25
<b>Index</b>	<b>27</b>



---

# Introduction to installing IBM Security QRadar Risk Manager

This information is intended for use with IBM® Security QRadar® Risk Manager. QRadar Risk Manager is an appliance used to monitor device configurations, simulate changes to your network environment, and prioritize risks and vulnerabilities in your network.

This guide contains instructions for installing QRadar Risk Manager and adding QRadar Risk Manager as a managed host on IBM Security QRadar SIEM console.

QRadar Risk Manager appliances are preinstalled with software and a Red Hat Enterprise Linux operating system. You can also install QRadar Risk Manager software on your own hardware.

## Intended audience

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

Administrators need a working knowledge of networking and Linux systems.

## Technical documentation

For information about how to access more technical documentation, technical notes, and release notes, see Accessing IBM Security Documentation Technical Note (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

## Contacting customer support

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

## Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



---

## Chapter 1. Prepare to install IBM Security QRadar Risk Manager

You can install an IBM Security QRadar Risk Manager appliance as a managed host on your IBM Security QRadar SIEM console. Only one QRadar Risk Manager can exist on a QRadar SIEM console.

As of version 7.1 of QRadar Risk Manager, QRadar SIEM and QRadar Risk Manager use the same installation process and ISO for installation. For this reason, you can use the deployment editor in QRadar SIEM to add QRadar Risk Manager to your deployment. A QRadar Risk Manager appliance installation includes the QRadar Risk Manager software and a Red Hat Enterprise Linux operating system.

---

### Before you install

You must complete the installation process for an IBM Security QRadar SIEM console before you install IBM Security QRadar Risk Manager. As a best practice, install QRadar SIEM and QRadar Risk Manager on the same network switch.

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

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

You must gather information about your network settings before starting the installation process.

Gather the following information for your network settings:

- Host name
- 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 that use Network Address Translation (NAT) email server name
- Email server name
- Network Time Protocol (NTP) server (Console only) or time server name

### Configure port access on firewalls

Firewalls between the IBM Security QRadar SIEM console and IBM Security QRadar Risk Manager must allow traffic on certain ports.

Ensure that any firewall 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 in QRadar Risk Manager

It is important to be aware of the features that are not supported by IBM Security QRadar Risk Manager.

The following features are not supported in QRadar Risk Manager:

- High availability (HA)
- Dynamic Routing for Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), or Routing Information Protocol (RIP)
- IPv6
- Non-contiguous network masks
- Load-balanced routes
- Reference maps
- Store and Forward

---

## Additional hardware requirements

Additional hardware is required before you can install IBM Security QRadar Risk Manager.

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

- monitor and keyboard or a serial console
- Uninterrupted Power<sup>®</sup> Supply (UPS)

QRadar Risk Manager appliances or systems that are running QRadar Risk Manager software that store data must be equipped with an Uninterrupted Power Supply (UPS). Using a UPS ensures that your QRadar Risk Manager data, such as consoles, event processors, and QFlow Collectors, is preserved during a power failure.

---

## Additional software requirements

Additional software is required before you can install IBM Security QRadar Risk Manager.

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

- Java<sup>™</sup> runtime environment
- Adobe Flash, version 10 or higher

---

## Supported web browsers

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

When you access the QRadar system, you are prompted for a user name and a password. The user name and password must be configured in advance by the administrator.



The following tables list the supported versions of web browsers.

*Table 1. Supported web browsers for QRadar products*

<b>Web browser</b>	<b>Supported version</b>
Mozilla Firefox	<ul style="list-style-type: none"><li>• 10.0 Extended Support Release (ESR)</li><li>• 10.0 Extended Support Release (ESR)</li></ul>
Microsoft Internet Explorer, with document mode and browser mode enabled	<ul style="list-style-type: none"><li>• 9.0</li></ul>
Google Chrome	<ul style="list-style-type: none"><li>• Latest version</li></ul>

## **Enabling document mode and browser mode in Internet Explorer**

If you use Microsoft Internet Explorer to access IBM Security QRadar products, you must enable browser mode and document mode.

### **Procedure**

1. In your Internet Explorer web browser, press F12 to open the Developer Tools window.
2. Click **Browser Mode** and select the version of your web browser.
3. Click **Document Mode** and select **Internet Explorer 7.0 Standards**.



---

## Chapter 2. Install IBM Security QRadar Risk Manager appliances

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

Installing QRadar Risk Manager involves the following steps:

1. Preparing your appliance.
2. Installing QRadar Risk Manager.
3. Adding QRadar Risk Manager to QRadar SIEM.

---

### Preparing your appliance

You must prepare your appliance before you install an IBM Security QRadar Risk Manager appliance.

#### Before you begin

You must install all necessary hardware and you need an activation key. The activation key is a 24-digit, four-part, alphanumeric string that you receive from IBM. 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.

To avoid typing errors, the letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

If you do not have an activation key for your QRadar Risk Manager appliance, contact customer support (<http://www.ibm.com/support>).

For information about your appliance, see the *IBM Security QRadar Hardware Installation Guide*.

#### Procedure

1. Choose one of the following options:
  - Connect a notebook to the serial port on the rear of the appliance.  
If you use a notebook to connect to the system, you must use a terminal program, such as HyperTerminal, to connect to the system. Make sure that 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.
2. Power on the system and login. The username, which is case-sensitive, is root.
3. Press Enter.
4. Read the information in the window. Press the Spacebar to advance each window until you reach the end of the document.
5. Type yes to accept the agreement, and then press Enter.
6. Type your activation key and press Enter.

---

## Access the IBM Security QRadar Risk Manager user interface

IBM Security QRadar Risk Manager uses default login information for the URL, user name, and password.

You access IBM Security QRadar Risk Manager through the QRadar SIEM console. Use the information in the following table when you log in to your IBM Security QRadar SIEM console.

*Table 2. Default login information for QRadar Risk Manager*

Login information	Default
URL	https://<IP address>, where <IP address> is the IP address of the QRadar SIEM console.
User name	admin
Password	The password that is assigned to QRadar Risk Manager during the installation process.
License key	A default license key provides access to the system for 5 weeks.

---

## Network parameter information for IPv4

Network information for Internet Protocol version 4 (IPv4) network settings is required when you install IBM Security QRadar Risk Manager or when you change network settings.

Use the information in the following table when you install or reinstall IBM Security QRadar Risk Manager, or when you need to change network settings.

*Table 3. Network information required for IBM Security QRadar Risk Manager installation*

Network information	Description
Email server	Type the name of the email server. If you do not have an email server, type localhost in this field.
Gateway	Type the default gateway of the system.
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.
Primary DNS	Type the primary DNS server address.
Public IP	Optional. Type the Public IP address of the server.  This secondary IP address 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 the 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.

---

## Installing IBM Security QRadar Risk Manager

You can install IBM Security QRadar Risk Manager after you prepare your appliance.

### Before you begin

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

### Procedure

1. Select normal for the type of setup. Select **Next** and press Enter.
2. Select your time zone continent or area. Select **Next** and press Enter.
3. Select your time zone region. Select **Next** and press Enter.
4. Select an Internet Protocol version. Select **Next** and press Enter.
5. Select the interface that you want to specify as the management interface. Select **Next** and press Enter.
6. Type your hostname, IP address, network mask, gateway, primary DNS, secondary DNS, public IP, and email server. For network parameter information, see “Network parameter information for IPv4” on page 6.
7. Select **Next** and press Enter.
8. Type a password to configure the QRadar Risk Manager root password.
9. Select **Next** and press Enter.
10. Retype your new password to confirm. Select **Finish** and press Enter. This process typically takes several minutes.

### What to do next

Use the deployment editor to add QRadar Risk Manager as a managed host to your QRadar SIEM console.

---

## Adding QRadar Risk Manager to QRadar SIEM

You must add IBM Security QRadar Risk Manager as a managed host to IBM Security QRadar SIEM.

### Before you begin

If you want to enable compression, then the minimum version for each managed host must be QRadar SIEM 7.1 or QRadar Risk Manager 7.1.

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

### Procedure

1. Open your web browser.
2. Type the URL, `https://<IP Address>`, where <IP Address> is the IP address of the QRadar SIEM console.
3. Type your user name and password.
4. On the **Admin** tab, click **Deployment Editor**.
5. From the menu, select **Actions**, and then select **Add a Managed Host**.

6. Click **Next**.

7. Enter values for the following parameters:

Option	Description
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 <i>IBM Security QRadar SIEM Administration Guide</i> .
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.

8. Choose one of the following options:

- If you selected the **Host is NATed** check box, then you must enter values for the NAT parameters.

Option	Description
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 that use NAT.
Select NATed network	From the list box, select the network that you want this managed host to use.  If the managed host is on the same subnet as the QRadar SIEM console, select the console of the NATed network.  If the managed host is not on the same subnet as the QRadar SIEM console, select the managed host of the NATed network.

- If you did not select the **Host is NATed** check box, click **Next**.

9. Click **Finish**. This process can take several minutes to complete. If your deployment includes changes, then you must deploy all changes.

10. Click **Deploy**.

## What to do next

Clear your web browser cache and then log in to QRadar SIEM. The **Risks** tab is now available.

---

## Clearing web browser cache

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

### Before you begin

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

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

### Procedure

1. Open your web browser.
2. Clear your web browser cache. For instructions, see your web browser documentation.

---

## Risk Manager user role

You must assign the Risk Manager user role for users that requires access to the **Risks** tab.

A user account defines the , default password, and email address for a user. You need to assign a user role and security profile for each new user account.

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.

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

## Assigning the Risk Manager user role

You can assign the Risk Manager user role for users that need access to the **Risk** tab.

### Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. In the **User Management** pane, click the **User Roles** icon.
4. Click the **Edit** icon next to the user role you want to edit.
5. Select the **Risk Manager** check box.
6. Click **Next**. If you add Risk Manager to a user role that has Log Activity permission, then you must define the log sources that 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.
7. Click **Return**.
8. From the **Admin** tab menu, click **Deploy Changes**.

---

## Troubleshoot the Risks tab

You can troubleshoot if the **Risks** tab does not display properly or is inaccessible.

When the Risks tab is not displaying properly or is inaccessible, you remove and readd IBM Security QRadar Risk Manager as a managed host.

### Removing a managed host

You can remove your IBM Security QRadar Risk Manager managed host from IBM Security QRadar SIEM to change network settings or if there is a problem with the **Risks** tab.

#### Procedure

1. Open your web browser.
2. Type the URL `https://<IP Address>`, where <IP Address> is the IP address of the QRadar SIEM console.
3. Type your user name and password.  
For default login information, see Table 2 on page 6
4. On the **Admin** tab, click **Deployment Editor**.
5. Click the **System View** tab.
6. Right-click the managed host that you want to delete and select **Delete**. Repeat for each non-Console managed host until all hosts are deleted.
7. Click **Save**.
8. Close the deployment editor.
9. On the **Admin** tab, click **Deploy Changes**.

#### What to do next

Readd QRadar Risk Manager as a managed host.

### Readd QRadar Risk Manager as a managed host

You can readd QRadar Risk Manager as a managed host after it is removed.

#### Procedure

1. Open your web browser.
2. Type the URL `https://<IP Address>`, where <IP Address> is the IP address of the QRadar SIEM console.
3. Type your user name and password.  
For default login information, see Table 2 on page 6
4. On the **Admin** tab, click **Deployment Editor**.
5. Click the **System View** tab.
6. From the menu, select **Actions > Add a managed host**.
7. Click **Next**.
8. Enter values for the following parameters:

Option	Description
Enter the IP of the QRadar Risk Manager appliance	Type the IP address of your QRadar Risk Manager appliance.



Option	Description
Enter the root password of the host	Type the root password for QRadar Risk Manager.
Confirm the root password of the host	Type the root password again, to confirm.
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.

9. Click **Next**.
10. Click **Finish**. The process of adding QRadar Risk Manager can take several minutes to complete.
11. Close the deployment editor.
12. On the **Admin** tab, click **Deploy Changes**.

## Results

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



---

## Chapter 3. Reinstall QRadar from the recovery partition

When you reinstall 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. This means that your current configuration and data files are overwritten.

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 reinstall QRadar Risk Manager, which restores QRadar Risk Manager to factory defaults.

**Note:** If you upgrade your software after you install QRadar Risk Manager, then the ISO file is replaced with the newer version.

When you reboot your QRadar Risk Manager appliance, you are presented with the option to reinstall the software. Since QRadar SIEM and QRadar Risk Manager use the same ISO installation file, the QRadar SIEM ISO name displays.

If you do not respond to the prompt after 5 seconds, the system reboots as normal, which maintains your configuration and data files. If you choose to reinstall QRadar SIEM ISO, a warning message is displayed and you must confirm that you want to reinstall the software. After confirmation, the installer runs and you can follow the prompts through the installation process.

After a hard disk failure, you cannot reinstall from the recovery partition because it is no longer available. If you experience a hard disk failure, contact Customer Support for assistance.

---

### Reinstalling QRadar Risk Manager by using Factory re-install

You can reboot and reinstall your QRadar Risk Manager appliance using the factory reinstall option.

#### Before you begin

Ensure that you have your activation key, which is a 24-digit, four-part, alphanumeric string that you receive from IBM. 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.

To avoid typing errors, the letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

If you do not have an activation key for your QRadar Risk Manager appliance, contact customer support (<http://www.ibm.com/support>).

Software activation keys do not require serial numbers.

## Procedure

1. Reboot your QRadar Risk Manager appliance.
2. Select **Factory re-install**.
3. Type **flatten** to continue. The hard disk is partitioned and reformatted, the OS is installed, and then QRadar Risk Manager is reinstalled. You must wait for the flatten process to complete. This process can take up to several minutes, depending on your system.
4. Type **SETUP**.
5. Log in to QRadar Risk Manager as the root user.
6. Read the information in the window. Press the Spacebar to advance each window until you reach the end of the document. Type **yes** to accept the agreement, and then press Enter.
7. Type your activation key and press Enter.
8. Select **normal** for the type of setup. Select **Next** and press Enter.
9. Select your time zone continent or area. Select **Next** and press Enter.
10. Select your time zone region. Select **Next** and press Enter.
11. Select an Internet Protocol version. Select **Next** and press Enter.
12. Select the interface that you want to specify as the management interface. Select **Next** and press Enter.
13. Enter information for your hostname, IP address, network mask, gateway, primary DNS, secondary DNS, public IP, and email server. For network information, see “Network parameter information for IPv4” on page 6.
14. Type your password to configure the QRadar Risk Manager root password.
15. Select **Next** and press Enter.
16. Retype your new password to confirm. Select **Finish** and press Enter. This process typically takes several minutes.
17. Press Enter to select OK.
18. Press Enter to select OK.

## What to do next

Use the deployment editor to add QRadar Risk Manager as a managed host to your QRadar SIEM console.

---

## Chapter 4. Change network settings

You can change the network settings of an IBM Security QRadar Risk Manager appliance that is attached to an IBM Security QRadar SIEM Console.

If you need to change the network settings, then you must complete these tasks in the following order:

1. Remove QRadar Risk Manager as a managed host.
2. Change network settings.
3. Readd QRadar Risk Manager as a managed host.

---

### Removing a managed host

You can remove your IBM Security QRadar Risk Manager managed host from IBM Security QRadar SIEM to change network settings or if there is a problem with the **Risks** tab.

#### Procedure

1. Open your web browser.
2. Type the URL `https://<IP Address>`, where `<IP Address>` is the IP address of the QRadar SIEM console.
3. Type your user name and password.  
For default login information, see Table 2 on page 6
4. On the **Admin** tab, click **Deployment Editor**.
5. Click the **System View** tab.
6. Right-click the managed host that you want to delete and select **Delete**. Repeat for each non-Console managed host until all hosts are deleted.
7. Click **Save**.
8. Close the deployment editor.
9. On the **Admin** tab, click **Deploy Changes**.

#### What to do next

Readd QRadar Risk Manager as a managed host.

---

### Change network settings

You can change the network settings of an IBM Security QRadar Risk Manager appliance that is attached to an IBM Security QRadar SIEM Console.

#### Before you begin

You must remove the QRadar Risk Manager managed host from QRadar SIEM before you change the network settings.

#### Procedure

1. Using SSH, log in to QRadar Risk Manager as the root user.
2. Type the command, `qchange_netsetup`.

3. Select an Internet Protocol version. Select **Next** and press Enter. Depending on your hardware configuration, the window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.
4. Select the interface that you want to specify as the management interface. Select **Next** and press Enter.
5. Enter information for your hostname, IP address, network mask, gateway, primary DNS, secondary DNS, public IP, and email server. For network information, see “Network parameter information for IPv4” on page 6.
6. Type your password to configure the QRadar Risk Manager root password.
7. Select **Next** and press Enter.
8. Retype your new password to confirm. Select **Finish** and press Enter. This process typically takes several minutes.

---

## Readd QRadar Risk Manager as a managed host

You can readd QRadar Risk Manager as a managed host after it is removed.

### Procedure

1. Open your web browser.
2. Type the URL `https://<IP Address>`, where <IP Address> is the IP address of the QRadar SIEM console.
3. Type your user name and password.  
For default login information, see Table 2 on page 6
4. On the **Admin** tab, click **Deployment Editor**.
5. Click the **System View** tab.
6. From the menu, select **Actions > Add a managed host**.
7. Click **Next**.
8. Enter values for the following parameters:

Option	Description
<b>Enter the IP of the QRadar Risk Manager appliance</b>	Type the IP address of your QRadar Risk Manager appliance.
<b>Enter the root password of the host</b>	Type the root password for QRadar Risk Manager.
<b>Confirm the root password of the host</b>	Type the root password again, to confirm.
<b>Host is NATed</b>	Select this option if you want to specify NAT values if necessary.
<b>Enable Encryption</b>	Select this option if you want to enable encryption.

9. Click **Next**.
10. Click **Finish**. The process of adding QRadar Risk Manager can take several minutes to complete.
11. Close the deployment editor.
12. On the **Admin** tab, click **Deploy Changes**.

## Results

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





---

## Chapter 5. Data back up and restore

You can use a command-line interface (CLI) script to back up data that is stored on IBM Security QRadar SIEM managed hosts.

You can use the CLI script to restore IBM Security QRadar Risk Manager after a data failure or hardware failure on the appliance.

A backup script is included in QRadar Risk Manager, which can be scheduled by using crontab. The script automatically creates a daily archive of QRadar Risk Manager data at 3:00 AM. By default, QRadar Risk Manager keeps the last five backups. If you have network or attached storage, you must create a cron job to copy QRadar Risk Manager back archives to a network storage location.

The backup archive includes the following data:

- QRadar Risk Manager device configurations
- Connection data
- Topology data
- Policy Monitor questions
- QRadar Risk Manager database tables

For information about migrating from QRadar Risk Manager Maintenance Release 5 to this current release, see the *IBM Security QRadar Risk Manager Migration Guide*.

---

### Prerequisites for backing up and restoring data

You must understand how data is backed up, stored, and archived before you back up and restore your data.

#### Data backup location

Data is backed up in the `/store/qrm_backups` local directory. Your system might include a mount `/store/backup` from an external SAN or NAS service. External services provide long term offline retention of data. Long-term storage might be required for compliancy regulations, such as Payment Card Industry (PCI) standards.

#### Appliance version

The version of the appliance that created the backup in the archive is stored. A backup can only be restored in a QRadar Risk Manager appliance if it is the same version.

#### Data backup frequency and archival information

Daily data backups are created at 3:00 AM. Only the last five backup files are stored. A backup archive is created if there is enough free space on QRadar Risk Manager.

## Format of backup files

Use the following format to save backup files: 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>.

---

## Backing up your data

Automatic backup occurs daily, at 3:00 AM, or you can start the backup process manually.

### Procedure

1. Using SSH, log in your QRadar SIEM console as the root user.
2. Using SSH from the QRadar SIEM console, log in to QRadar Risk Manager as the root user.
3. Start a QRadar Risk Manager backup by typing `/opt/qradar/bin/dbmaint/risk_manager_backup.sh`

### Results

The script that is used to start the backup process might take several minutes to start.

After the script completes the backup process, 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
```

---

## Restoring data

You can use a restore script to restore data from a QRadar Risk Manager backup.

### Before you begin

The QRadar Risk Manager appliance and the backup archive must be the same 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.

### About this task

Use the restore script to specify the archive that you are restoring to QRadar Risk Manager. This process requires you to stop services on QRadar Risk Manager. Stopping services logs off all QRadar Risk Manager users and stops multiple processes.

The following table describes the parameters that you can use to restore a backup archive.

Table 4. Parameters used to restore a backup archive to QRadar Risk Manager

Option	Description
<b>-f</b>	Overwrites any existing QRadar Risk Manager data on your system with the data in the restore file. Selecting this parameter allows the script to overwrite any existing device configurations in Configuration Source Management with the device configurations from the backup file.
<b>-w</b>	Do not delete directories before you restore QRadar Risk Manager data.
<b>-h</b>	The help for the restore script.

## Procedure

1. Using SSH, log in your QRadar SIEM console as the root user.
2. Using SSH from the QRadar SIEM console, log in to QRadar Risk Manager as the root user.
3. Stop hostcontext by typing `service hostcontext stop`.
4. Type the following command to restore a backup archive to QRadar Risk Manager: `/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, `backup-2012-09-11-10-14-39.tgz`.
5. Start hostcontext by typing `service hostcontext start`.



---

## 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://ibm.com)<sup>®</sup> are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (<sup>®</sup> or <sup>™</sup>), these symbols

indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information ([www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)).

Adobe and Acrobat and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a 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.

Other company, product, and service names may be trademarks or service marks of others.

---

## Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at <http://www.ibm.com/privacy> and IBM’s Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at <http://www.ibm.com/software/info/product-privacy>.





---

## Index

### A

activation key 5  
add QRadar Risk Manager 7  
appliance preparation 5

### B

back up data 19  
browser mode  
    Internet Explorer web browser 3

### D

default log in information 6  
document mode  
    Internet Explorer web browser 3  
dynamic routing 2

### G

gateway address 1

### H

high availability (HA) 2

### I

install QRadar Risk Manager 7  
introduction v  
IP address 1  
IPv6 2

### L

log in information 6

### M

managed host 7

### N

network administrator v  
network information 1  
network mask address 1  
network setting changes 15  
non-contiguous network masks 2  
NTP server 1

### P

password 6  
port 22 1  
port 37 1  
port 443 1

port requirements 1  
preparing for installation 1, 5

### R

restore data 19  
Risk Manager user role 9

### S

security profile 9  
subnet mask 1

### U

unsupported features 2  
user name 6  
user role 9

### W

web browser  
    supported versions 2







Printed in USA