IBM Security QRadar Network Anomaly Detection
Version 7.1.0 (MR2)

Installation Guide

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 21.

CONTENTS

ABOUT THIS GUIDE

1 PREPARATION FOR YOUR INSTALLATION

2 INSTALLING QRADAR NETWORK ANOMALY DETECTION APPLIANCES

3 NETWORK SETTING MANAGEMENT

4 RE-INSTALLATION FROM THE RECOVERY PARTITION

A NOTICES AND TRADEMARKS

INDEX

ABOUT THIS GUIDE

The *IBM Security QRadar Network Anomaly Detection Installation Guide* provides you with information on installing QRadar Network Anomaly Detection 7.1 (MR1). QRadar Network Anomaly Detection appliances are pre-installed with software and a Red Hat Enterprise Linux version 6.3 operating system; however, you can install QRadar Network Anomaly Detection 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 Network Anomaly Detection systems in your network.

Documentation conventions

The following conventions are used throughout this guide:

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)

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.

1 PREPARATION FOR YOUR INSTALLATION

To ensure a successful IBM Security QRadar Network Anomaly Detection deployment, adhere to the preparation requirements and recommendations included in this topic.

QRadar Network Anomaly Detection deployment overview

QRadar Network Anomaly Detection deployment architecture allows you to install components on a single server for small enterprises or distributed across multiple servers for maximum performance and scalability in large enterprise environments.

QRadar Network Anomaly Detection components

QRadar Network Anomaly Detection deployments can include the following components:

- **QRadar QFlow Collector** - Passively collects traffic flows from your network through span ports or network taps. The QRadar QFlow Collector also supports the collection of external flow-based data sources, such as NetFlow. You can install a QRadar QFlow Collector on your own hardware or use one of the QRadar QFlow Collector appliances.
- **Console** - Provides the QRadar Network Anomaly Detection user interface, which provides real time event and flow views, reports, offenses, asset information, and administrative functionality. Using the Console, you can also manage hosts that include other components in a distributed QRadar Network Anomaly Detection deployment.
- **Event Collector** - Gathers events from local and remote log sources. The Event Collector normalizes raw log source events. During this process, the Magistrate component examines the event from the log source and maps the event to a IBM Security QRadar Identifier (QID). Then the Event Collector bundles identical events to conserve system usage and sends the information to the Event Processor.
- **Event Processor** - Processes events collected from one or more Event Collector. The Event Processor correlates the information from QRadar Network Anomaly Detection and distributes the information to the appropriate area, depending on the type of event. The Event Processor also includes information gathered by QRadar Network Anomaly Detection to indicate

behavioral changes or policy violations for the event. When complete, the Event Processor sends the events to the Magistrate component.

- **Magistrate** - Provides the core processing components. You can add one Magistrate component for each deployment. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events. The Magistrate processes events against the custom rules. If an event matches a rule, the magistrate generates the response configured in the custom rule. For example, the custom rule may indicate that when an event matches the rule, an offense is created. If there is no match to a custom rule, the Magistrate uses default rules to process the event. An offense is an alert that has been processed using multiple inputs, individual events, and events combined with analyzed behavior and vulnerabilities. The magistrate prioritizes the offenses and assigns a magnitude value based on several factors, including number of events, severity, relevance, and credibility.

For more information on each QRadar Network Anomaly Detection component, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Additional hardware requirements

Before you install QRadar Network Anomaly Detection systems, make sure you have access to the following hardware components:

- Monitor and keyboard, or a serial console
- Uninterrupted Power Supply (UPS) for all systems that store data, such as Consoles, Event Processors, or QRadar QFlow Collectors
- Null modem cable if you want to connect the system to a serial console

Additional software requirements

Before you install QRadar Network Anomaly Detection, make sure you have the following applications installed on any desktop system that you use to access the QRadar Network Anomaly Detection user interface:

- Java^{TM} Runtime Environment (JRE)
- Adobe Flash 10.x

You can download Java 1.6.0_u24 at the following website: *http://java.com/*. Make sure that you install JRE on your desktop system, not on the QRadar Network Anomaly Detection system.

Supported browsers

You can access the Console from a standard web browser. When you access the system, a prompt asks for a user name and a password, which must be configured in advance by the QRadar Network Anomaly Detection 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 test the latest versions of the Mozilla Firefox browser. However, we are fully committed to investigate 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 use the Microsoft Internet Explorer web browser, you must enable Compatibility View.

Procedure

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.**

Required network settings

Before you install QRadar Network Anomaly Detection, you must identify the following information for each system that you want to install:

- Hostname
- IP address
- Network mask address
- Subnet mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (optional)

- Public IP address for networks using Network Address Translation (NAT)
- Email server name
- Network Time Protocol (NTP) server (Console only) or time server name

2 INSTALLING QRADAR NETWORK ANOMALY DETECTION APPLIANCES

Use the procedures in this topic to install an IBM Security QRadar Network Anomaly Detection Console. QRadar Network Anomaly Detection appliances include QRadar Network Anomaly Detection software and a Red Hat Enterprise Linux operating system.

For more information about appliances, see the *Hardware Installation Guide*.

Preparing your QRadar Network Anomaly Detection appliance for installation

Before you can use the installation wizard to install a QRadar Network Anomaly Detection appliance, you must physically install and prepare the appliance.

About this task

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).

For more information on your QRadar Network Anomaly Detection appliance, see the *Hardware Installation Guide*.

Procedure

Step 1 Install all necessary hardware.

Step 2 Choose one of the following options:

- Connect a laptop to the serial port on the rear of the appliance.
- Connect a keyboard and monitor to their respective ports.

Step 3 Power on the system and log in:

Username: **root**

Note: The username is case sensitive.

Step 4 Press Enter.

What to do next

Installing a QRadar Network Anomaly Detection Console

Installing a QRadar Network Anomaly Detection Console

Use this procedure to install a QRadar Network Anomaly Detection Console.

Before you begin

Before you begin, ensure that the following requirements are met:

- Your appliance is prepared for installation. If your appliance is not prepared for installation, see **Preparing your QRadar Network Anomaly Detection appliance for installation**.
- The End User License Agreement (EULA) window is displayed.
- Locate your activation key. The activation key is a 24-digit, four-part, alphanumeric string that you receive from IBM. The letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

About this task

When you read the End User License Agreement (EULA), press the Spacebar to advance each window until you reach the end of the document.

The Internet Protocol Version window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

When you configure the network settings, you can configure a public IP address for 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.

When you create the root password, the password must meet the following criteria:

- Must contain at least five characters
- No spaces
- Can include the following special characters: @,#,^, and *.

Procedure

Step 1 Read the information in the End User License Agreement (EULA) window.

Step 2 Type **yes** to accept the agreement, and then press Enter.

Step 3 Type your activation key and press Enter.

Step 4 Select **normal** for the type of setup. Select **Next** and press Enter.

Step 5 Select the **Enterprise** tuning template. Select **Next** and press Enter.

Step 6 Configure your time settings:

a Choose one of the following options:

- **Manual** - Select this option to manually input the time and date. Select **Next** and press Enter. The Current Date and Time window is displayed. Go to b.

- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **c**.

b To manually enter the time and date, type the current time and date. Select **Next** and press Enter. Go to **Step 7**.

c To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter. Go to **Step 9**.

Step 7 On the Time Zone Continent window, select your time zone continent or area. Select **Next** and press Enter.

Step 8 On the Time Zone Region window, select your time zone region. Select **Next** and press Enter.

Step 9 Select an internet protocol version. Select **Next** and press Enter.

Step 10 Select the interface that you want to use as the management interface. Select **Next** and press Enter.

Step 11 Choose one of the following options:

- If you use IPv4 as your Internet protocol, go to **Step 14**.
- If you use IPv6 as your Internet protocol, go to **Step 12**.

Step 12 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 14**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 13**.

Step 13 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 15**.

Step 14 Configure the QRadar Network Anomaly Detection 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.
- **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 15 Configure the QRadar Network Anomaly Detection root password:

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

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

Step 16 Press Enter to select **OK**.

Result

After you configure the installation parameters, a series of messages are displayed as QRadar Network Anomaly Detection continues with the installation. This process typically takes several minutes.

What to do next

See **Accessing the QRadar Network Anomaly Detection user interface**.

Accessing the QRadar Network Anomaly Detection user interface

After the installation is complete, you can access the QRadar Network Anomaly Detection user interface.

About this task

When you access the QRadar Network Anomaly Detection for the first time, note the following requirements:

- If you use Mozilla Firefox, you must add an exception to Mozilla Firefox. For more information, see your Mozilla documentation.
- If you use Internet Explorer, a website security certificate message is displayed. You must select the Continue to this website option to log in to QRadar Network Anomaly Detection.
- For your QRadar Network Anomaly Detection Console, a default license key provides you access to QRadar Network Anomaly Detection for five weeks. For more information on the license key, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Procedure

Step 1 Open your web browser.

Step 2 Log in to QRadar Network Anomaly Detection:

```
https://<IP Address>
```

Where <`IP Address`> is the IP address of the QRadar Network Anomaly Detection system. The default values are:

Username: `admin`

Password: `<root password>`

Step 3 Click **Login To QRadar Network Anomaly Detection**.

3 NETWORK SETTING MANAGEMENT

Use the `qchange_netsetup script` to change the network settings of your IBM Security QRadar Network Anomaly Detection system. Configurable network settings include hostname, IP address, network mask, gateway, DNS addresses, public IP address, and email server.

Changing the network settings

You can change the network settings in your all-in-one system. An all-in-one system has all QRadar Network Anomaly Detection components, including the **Admin** tab, installed on one system.

Before you begin

You must have a local connection to your Console before you start this procedure.

About this task

The Internet Protocol Version window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

When you configure the network settings, you can configure a public IP address for 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.

Procedure

Step 1 Log in to QRadar Network Anomaly Detection 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.

Step 4 Select the interface that you want to use as the management interface. Select **Next** and press Enter.

Step 5 Choose one of the following options:

- If you use IPv4 as your Internet protocol, go to **Step 8**.
- If you use 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 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 Network Anomaly Detection 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.
- **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.

Result

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

Updating network settings after a NIC replacement

If you perform a replacement of your integrated motherboard or stand-alone NICs, you must update your QRadar Network Anomaly Detection network settings to ensure your hardware remains operational.

About this task

This task involves the network settings file. The file displays one pair of lines for each NIC that has been installed and one pair of lines for each NIC that has been removed. You must remove the lines for the NIC that you removed and then rename the NIC that you installed.

Your network settings file may resemble the following example:

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"


# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"


# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4"


# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4"
```

Where **`NAME=″eth0″`** is the NIC that was replaced and **`NAME=″eth4″`** is the NIC that was installed.

Procedure

Step 1 Using SSH, log in to QRadar Network Anomaly Detection as the root user:

Username: **root**

Password: **<password>**

Step 2 Type the following command:

```
cd /etc/udev/rules.d/
```

Step 3 To edit the network settings file, type the following command:

```
vi 70-persistent-net.rules
```

Step 4 Remove the pair of lines for the NIC which has been replaced; **`NAME=″eth0″`**.

Step 5 Rename the **`Name=<eth>`** values for the newly installed NIC. For example, **`NAME="eth4"`** should be renamed to **`NAME="eth0"`**.

Step 6 Save and close the file.

Step 7 Type the following command:

```
reboot
```

4 RE-INSTALLATION FROM THE RECOVERY PARTITION

If required, you can re-install IBM Security QRadar Network Anomaly Detection software from the recovery partition. This section applies to new QRadar Network Anomaly Detection 7.1 (MR2) installations or upgrades from new QRadar Network Anomaly Detection 7.0 installations on QRadar appliances.

Recovery partition overview

When you install QRadar Network Anomaly Detection, the installer (ISO) is copied into the recovery partition. From this partition, you can re-install QRadar Network Anomaly Detection, which restores your system to factory defaults. Your system is restored back to factory default configuration. Your current configuration and data files are overwritten.

When you reboot your QRadar Network Anomaly Detection appliance, you are presented with the option to re-install the software. If you do not respond to the prompt after 5 seconds, the system reboots as normal, thus your configuration and data files are maintained. If you choose the re-install QRadar Network Anomaly Detection option, a warning message is displayed and you must confirm that you want to re-install QRadar Network Anomaly Detection. After confirmation, the installer runs and you can follow the prompts through the installation process.

Note: 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.

Any software upgrades you perform after you install QRadar Network Anomaly Detection 7.1 (MR2) replaces the ISO file with the newer version.

Re-installing QRadar Network Anomaly Detection from the recovery partition

This topic provides the procedure for re-installing QRadar Network Anomaly Detection from the recovery partition.

Before you begin

Before you begin, ensure that the following requirements are met:

- Locate your 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.

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 your activation key, contact the Welcome Center at *welcomecenter@q1labs.com* or or *http://www.ibm.com/support* with the serial number of the QRadar Network Anomaly Detection appliance. Software activation keys do not require serial numbers

About this task

When you read the End User License Agreement (EULA), press the Spacebar to advance each window until you reach the end of the document.

The Internet Protocol Version window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

When you configure the network settings, you can configure a public IP address for 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.

When you create the root password, the password must meet the following criteria:

- Must contain at least five characters
- No spaces
- Can include the following special characters: @,#,^, and *.

When you type `flatten` during the procedure, the installer partitions and reformats the hard disk, installs the OS, and then re-installs QRadar Network Anomaly Detection. You must wait for the flatten process to complete. This process can take up to several minutes. When the process is complete, a confirmation is displayed.

Procedure

Step 1 Reboot your QRadar Network Anomaly Detection appliance.

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

Step 3 Type `flatten` to continue.

Step 4 Type `SETUP`.

Step 5 Log in to QRadar Network Anomaly Detection as the root user.

Username: root

Password: <password>

Step 6 Read the information in the End User License Agreement (EULA) window.

Step 7 Type your activation key and press Enter.

Step 8 If you are re-installing a non-Console appliance, go to **Step 11**.

Step 9 Select the **Enterprise** tuning template. Select **Next** and press Enter.

Step 10 Configure your time settings:

a Choose one of the following options:

- **Manual** - Select this option to manually input the time and date. Select **Next** and press Enter. The Current Date and Time window is displayed. Go to **b**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **c**.

b To manually enter the time and date, type the current time and date. Select **Next** and press Enter. Go to **Step 11**.

c To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter. Go to **Step 13**.

Step 11 On the Time Zone Continent window, select your time zone continent or area. Select **Next** and press Enter.

Step 12 On the Time Zone Region window, select your time zone region. Select **Next** and press Enter.

Step 13 Select an internet protocol version. Select **Next** and press Enter.

Step 14 Select the interface that you want to use as the management interface. Select **Next** and press Enter.

Step 15 Choose one of the following options:

- If you use IPv4 as your Internet protocol, go to **Step 18**.
- If you use IPv6 as your Internet protocol, go to **Step 16**.

Step 16 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 18**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 17**.

Step 17 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 19**.

Step 18 Configure the QRadar Network Anomaly Detection 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.
- **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 19 Configure the QRadar Network Anomaly Detection root password:

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

The password must meet the following criteria:

- Must contain at least five characters
- No spaces
- Can include the following special characters: @,#,^, and *.

The Confirm New Root Password window is displayed.

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

Step 20 Press Enter to select **OK**.

Result

After you configure the installation parameters, a series of messages are displayed as QRadar Network Anomaly Detection continues with the re-installation. This process typically takes several minutes.

What to do next

See **Accessing the QRadar Network Anomaly Detection user interface**

Accessing the QRadar Network Anomaly Detection user interface

After the installation is complete, you can access the QRadar Network Anomaly Detection user interface.

About this task

When you access the QRadar Network Anomaly Detection for the first time, note the following requirements:

- If you use Mozilla Firefox, you must add an exception to Mozilla Firefox. For more information, see your Mozilla documentation.
- If you use Internet Explorer, a website security certificate message is displayed. You must select the Continue to this website option to log in to QRadar Network Anomaly Detection.
- For your QRadar Network Anomaly Detection Console, a default license key provides you access to QRadar Network Anomaly Detection for five weeks. For

more information on the license key, see the *IBM Security QRadar Network Anomaly Detection Administration Guide*.

Procedure

Step 1 Open your web browser.

Step 2 Log in to QRadar Network Anomaly Detection:

```
https://<IP Address>
```

Where <`IP Address`> is the IP address of the QRadar Network Anomaly Detection system. The default values are:

Username: `admin`

Password: `<root password>`

Step 3 Click **Login To QRadar Network Anomaly Detection**.

A NOTICES AND TRADEMARKS

What's in this appendix:

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

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

Notices

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

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

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

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

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

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

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

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

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

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

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

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

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

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

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

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

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

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

Trademarks

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

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

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

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

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

INDEX