IBM Security QRadar
Version 7.1.0 (MR1)

FIPS Installation Guide

CONTENTS

ABOUT THIS GUIDE

The *IBM Security QRadar FIPS Installation Guide* provides you with information on installing and enabling FIPS mode for QRadar systems.

For specific information about IBM® Security products that are FIPS certified, consult the IBM Security FIPS 140 Security Policy documents. Find these documents on the National Institute of Standards and Technology (NIST) web site, in the Module Validation Lists section: *http://csrc.nist.gov/groups/STM/cmvp/index.html*.

Intended audience

This guide is intended for cryptographic operations users or administrators responsible for installing, maintaining, and configuring FIPS enabled QRadar systems in your network. The process of enabling FIPS mode allows you to create an admin user and crypto user role for general security services or cryptographic operations.

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.*

FIPS general requirements

It is important that you read the following general information about your IBM Security QRadar FIPS appliance:

- Use firmware that you know to be FIPS certified for FIPS compliance.

  For specific information about IBM Security products that are FIPS certified, consult the IBM Security FIPS 140 Security Policy documents. You can find these documents on the National Institute of Standards and Technology (NIST) website, in the Module Validation Lists section: *http://csrc.nist.gov/groups/STM/cmvp/index.html.*

- IBM Security QRadar uses the FIPS 140-2 approved cryptographic provider(s) for cryptography.

  The approved Cryptographic Security Kernel could be listed as Q1 Labs or Q1 Labs, an IBM Company, or IBM Corp. The certificates are listed on the NIST website: *http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm.*

- You must enable FIPS mode after your initial appliance installation and configuration.
- You must enable FIPS mode on any appliance that you restore to factory default (unconfigured) settings.

Appliance restrictions

It is important that you read and understand the following restrictions about your IBM Security QRadar FIPS appliance:

- It is not possible to SSH to an appliance with FIPS mode enabled using the root user account. Only the crypto user account or admin user accounts can SSH to a FIPS enabled QRadar appliance.
- It is not possible to install this appliance as a virtual machine (VM)
- Do not install software patches for QRadar appliances, unless the update is FIPS certified.
- It is not possible to disable FIPS mode through your browser using the QRadar user interface. The crypto user account is the only role with permissions to disable FIPS mode.
- Do not select MD5 or DES when configuring SNMP responses because these options are not FIPS-compliant. If these options are chosen while in FIPS mode, the appliance does not execute the response and it creates an error message in the system log. The error message states that the response is invalid.
- High-availability (HA) is not supported on FIPS appliances.

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 PREPARING YOUR APPLIANCE

This section is intended to instruction you on how to prepare your IBM Security QRadar FIPS appliance and apply tamper-proof labels before you rack-mount your appliance.

Safety notices

Safety guidelines help ensure your own personal safety and protect your system and working environment from potential damage.

You must read and understand these notices before you continue to install your hardware.

Systems are considered to be components in a rack. Thus, the term component refers to any system, various peripherals, or supporting hardware.

Observe the following precautions for rack stability and safety:

- System rack kits are intended to be installed in a rack by trained service technicians. Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.

WARNING: *Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack. After installing system/components in a rack, never pull more than one component out of the rack on the slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.*

Note: Your system is safety-certified as a free-standing unit and as a component for use in a rack cabinet using the customer rack kit. The installation of your system and rack kit in any other rack cabinet has not been approved by any safety agency. It is your responsibility to ensure that the final combination of system and rack complies with all applicable safety standards and local electric code requirements. IBM disclaims all liability and warranties in connection with such combinations.

WARNING: *Do not move racks by yourself. Due to the height and weight of the rack, a minimum of two people should accomplish this task.*

- Always load the rack from the bottom up and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the rails can pinch your fingers.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any component when servicing other components in a rack.

Additional hardware requirements

Before you install QRadar, ensure that you have access to the following hardware components:

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

  To ensure your QRadar data is preserved during a power failure, we recommend that all QRadar appliances be equipped with an Uninterrupted Power Supply (UPS).

Additional software requirements

Before you install QRadar, ensure that you have the following applications on the desktop system that is used to access QRadar:

- Java™ Runtime Environment (JRE) installed on the desktop system you plan to use to view QRadar.

  You can download Java 1.6.0_u24 from the following website: *http://java.com/*.
- Adobe Flash 10.x installed on the desktop you plan to use to access the QRadar Console.

Physical security

This section provides information on installing tamper-proof physical security labels to meet Security Level 2 FIPS compliance.

Two sets of twenty tamper-proof labels are included with your QRadar FIPS appliance for a total of forty (40) tamper-proof labels. These labels are numbered with a 7-digit code for your appliance.

Overview

Physical security labels are intended to overlap seams, service doors, and disk bays to prevent tampering with your QRadar FIPS appliance.

Sixteen (16) labels are required for FIPS physical security and must be installed before you place the appliance in the server rack. Any labels from installation steps marked as optional can be installed or saved for maintenance purposes.

The following list outlines the location and tamper-proof label quantity:

- Labels 1 and 2 (Qty 2) - Optional. Installed on top of the appliance.
- Labels 3 to 6 (Qty 4) - Required and installed on the sides of the appliance.
- Labels 7 and 8 (Qty 2) - Optional. Installed at the rear of the appliance.
- Labels 9 to 20 (Qty 12) - Required and installed covering hard drive bays.

If your appliance did not include labels for FIPS physical security or did not contain a sufficient number of labels, you must contact your sales representative to receive additional labels.

What to do next

You are now ready to install your tamper-proof labels. For more information, see **Installing tamper-proof labels**.

Installing tamper-proof labels

This procedure is intended to guide you when you install the tamper-proof labels for your QRadar FIPS appliance.

Procedure

Step 1 Ensure the location is free of dust or debris before installing a tamper-proof label.

Step 2 Optional. Apply two (2) labels on top of your FIPS appliance across the horizontal seam, as indicated.

The top labels 1 and 2 are optional and can be used as spare tamper-proof labels.

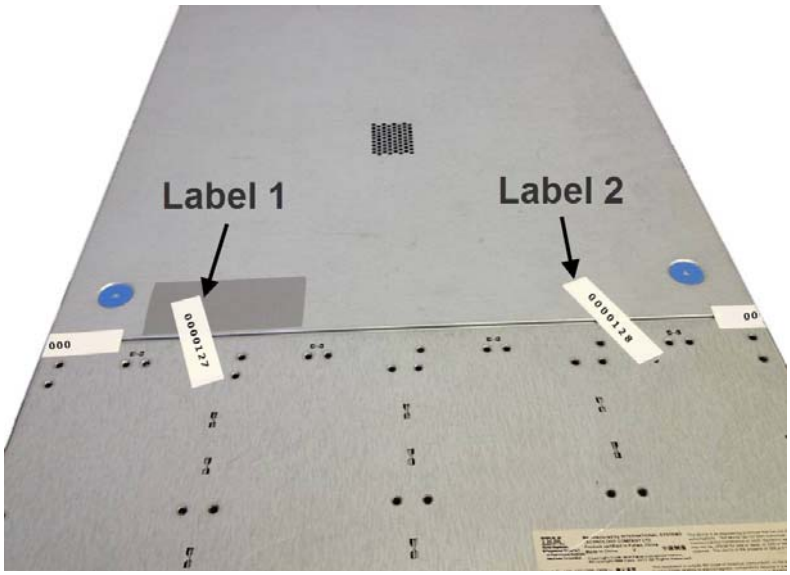

Figure 1-1 Optional labels 1 and 2 applied across the top seam of the appliance.

Step 3 Apply two (2) labels to cover the left and right side panel seam of your FIPS appliance, as indicated.

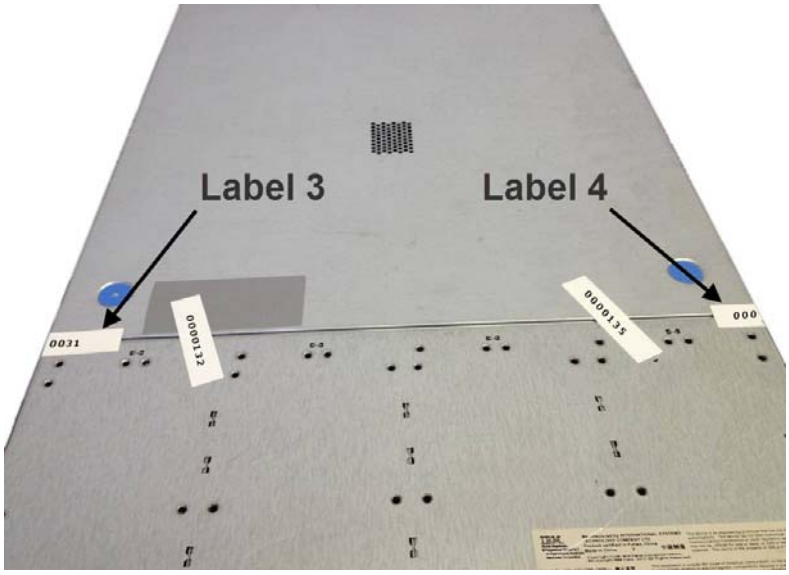

Figure 1-2 Labels 3 and 4 applied across the seam on the side of the appliance.

The label should cover the both edges of the seam and wrap to cover the side as shown in **Figure 1-3**.

Figure 1-3 Label 3 and 4 side installation.

Step 4 Apply two (2) labels on the side, near the back of the appliance, as indicated.

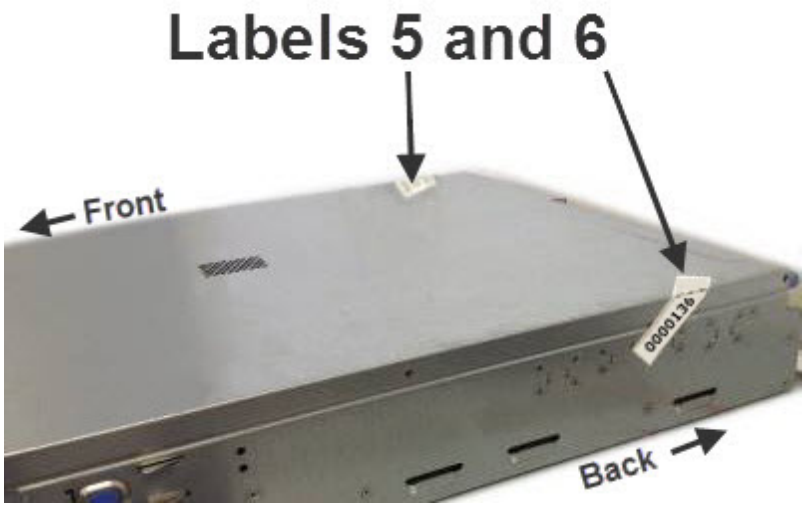

Figure 1-4 Labels 5 and 6 applied across the upper-left and upper-right side of the appliance.

Step 5 Optional. Apply two (2) labels at the rear of the appliance, as indicated.

The rear labels 7 and 8 are optional and can be used as spare tamper-proof labels.

Figure 1-5 Optional labels 7and 8 applied across the back of the appliance.

Step 6 Apply twelve (12) labels to cover the drive bays of your FIPS appliance, as indicated.

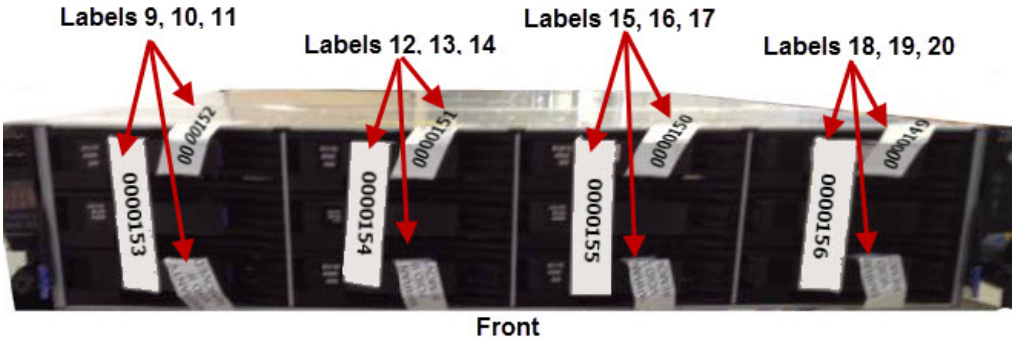

Figure 1-6 Tamper-proof labels applied to the hard drive bays.

Note: You must ensure that the labels wrap tightly to the top and bottom of the hard drive bays as shown in **Figure 1-7** and **Figure 1-8**.

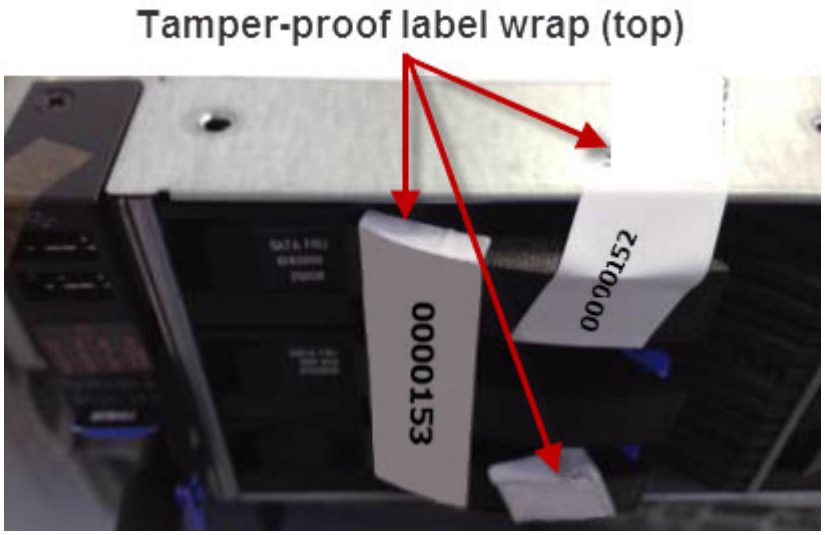

Figure 1-7 Tamper-proof labels wrapping over the drive bay latches.

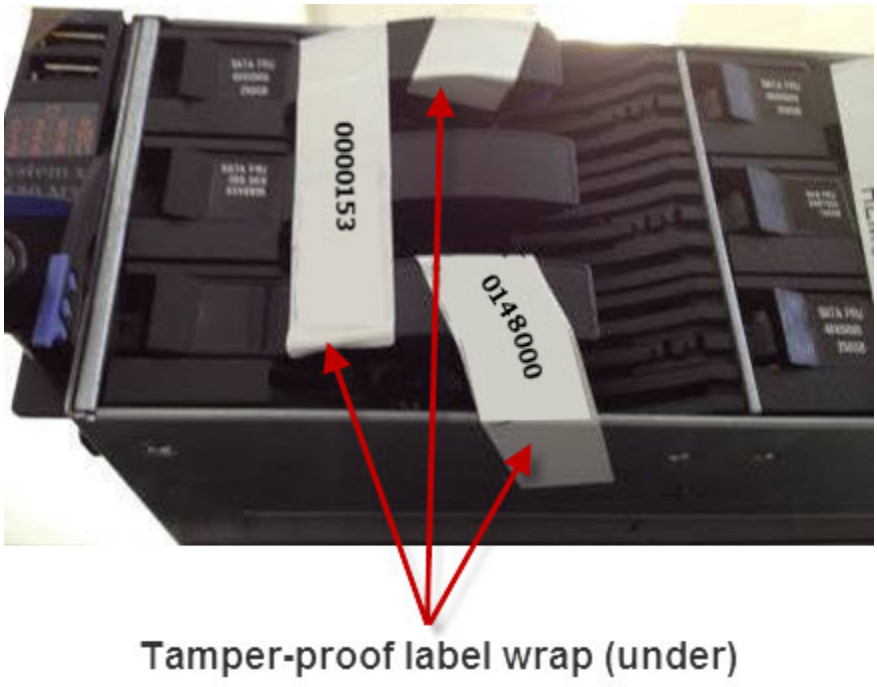

Figure 1-8 Tamper-proof labels wrapping under the drive bay latches.

Step 7 Review the placement of all tamper-proof labels to ensure that all labels are firmly attached.

The procedure is complete. You are now ready to continue installing your appliance.

Replacing a label

This procedure is intended to guide you when you need to replace a tamper-proof label for your QRadar FIPS appliance.

Procedure

Step 1 Remove any remnants of the previous tamper proof-label.

Step 2 Thoroughly clean the label location to remove any adhesive residue.

Rubbing alcohol or an alcohol swab can remove the adhesive residue.

Step 3 Replace the tamper-proof and complete any paper work required to note the maintenance on a FIPS appliance.

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 administrator.

Table 1-1 Supported Web Browsers

Web Browser	Supported Versions
Mozilla Firefox	• 10.0 Due to the short release cycles for Mozilla products, 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 **Enable Compatibility View for Microsoft Internet Explorer**.

Enable 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, you must gather the following information to plan your deployment for each FIPS 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 (optional) address
- Public IP address for networks with Network Address Translation (NAT)
- Email server name
- Network Time Protocol (NTP) server (Console only) or time server name

What to do next

You are now ready to install your QRadar appliance. For more information, see **Installing QRadar**.

2 INSTALLING QRADAR FIPS SOFTWARE

The installation of a QRadar FIPS appliance requires you to install your software, configure and add managed hosts, and enable FIPS mode.

Installing QRadar

You can use the following instruction to guide you through your QRadar FIPS appliance installation.

Procedure

Step 1 Prepare your appliance.

a Install the sixteen (16) required tamper-proof labels for FIPS compliance.

b Install all necessary hardware.

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

c Choose one of the following options:

- Connect a keyboard and monitor to their respective ports.
- 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).

d Power on the system and login:

User name: **`root`**

Note: The user name is case-sensitive.

e Press Enter.

The End User License Agreement (EULA) is displayed.

f Read the information in the window. Press the Spacebar to advance each page until you reach the end of the document.

g 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 with your FIPS appliance.

You can locate 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.

h Type the activation key and press Enter.

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

Step 2 Select **normal** for the type of setup. Select **Next** and press Enter.

Step 3 Select the **Enterprise** tuning template. Select **Next** and press Enter.

Step 4 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 **Step 5**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **Step 6**.

Step 5 To manually enter the time and date, type the current time and date. Select **Next** and press Enter. Go to **Step 9**.

Step 6 To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter.

Step 7 Select your time zone continent or area. Select **Next** and press Enter.

Step 8 Select your time zone region. Select **Next** and press Enter.

Step 9 Select an Internet Protocol version. Select **Next** and press Enter.

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

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

Step 11 Choose one of the following options:

- If you are using IPv4 as your Internet Protocol, go to **Step 14**.
- If you are using 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 amount of time. Go to **Step 14**.

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

Step 13 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 15**

Step 14 Configure the QRadar 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. The public IP address is a secondary address that is used to access the server, usually from a different network or the Internet. The Public IP address is often configured with Network Address Translation (NAT) services on your network or firewall settings on your 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 15 Configure the QRadar root password:

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

The password must meet the following criteria:

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

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

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

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

The installation is complete.

What to do next

You are now ready to configure any additional appliances that are managed by the QRadar FIPS Console. For more information, see **Setting up and configuring QRadar**.

Setting up and configuring QRadar

Before you enable FIPS mode on any of your appliances, you must set up your QRadar system and add any managed hosts.

Depending on your requirements, your organization can have your entire deployment in FIPS mode. All appliances in your FIPS deployment must be configured, added to the QRadar Console, then configured before you enable FIPS.

To set up your QRadar deployment:

1. Install all of your QRadar appliances.
2. Add any managed hosts with the deployment editor from the **Admin** tab of your QRadar Console.
3. Save and deploy your configuration update on your QRadar Console.

What to do next

You are now ready to enable FIPS mode on your appliances. For more information, see **Enabling FIPS mode**.

Enabling FIPS mode

Use the command-line interface to enable FIPS mode on your QRadar appliance.

When you enable FIPS mode on a QRadar appliance, command-line interface access is restricted to the admin role or crypto user accounts. These accounts are created when you enable FIPS mode for QRadar. SSH access is restricted to the FIPS admin and crypto user accounts. Enabling FIPS on your QRadar appliance guides you through the process of creating the admin and crypto user accounts.

You must enable FIPS in the following order for your appliances:

1. Managed hosts
2. QRadar Console

Procedure

Step 1 Using SSH, log in to QRadar as a root user.

Step 2 Type the following command:

```
/opt/qradar/fips/setup/fips_setup.py --enable
```

If any required cryptographic files are missing, the output alerts you to the missing files.

Step 3 Type **Yes** to enable FIPS mode.

Step 4 Type a password for the crypto user account. The password must meet the following criteria:

- Must contain at least six characters.
- Must include one special character, such as a period, comma, $, !, %, ^, or *.

Step 5 Retype the crypto password to confirm.

Step 6 Type a password for the admin user account. The password must meet the following criteria:

- Must contain at least six characters
- Must include one special character, such as a period, comma, $, !, %, ^, or *.

Step 7 Retype the admin password to confirm.

Step 8 Type **reboot** to restart your QRadar appliance.

After the appliance restarts services, FIPS mode is enabled.

You must repeat this process to enable FIPS mode on each additional managed host in your deployment. The QRadar Console is the final appliance that you enable in FIPS mode.

What to do next

You are now ready to disable automatic updates on your FIPS appliances. For more information, see **Disabling automatic updates**.

Disabling automatic updates

To prevent your system from automatically installing software updates, you must disable software updates on your QRadar Console.

The FIPS specification requires that you install FIPS-certified and tested software. However, Device Support Modules (DSMs), protocols, and scanner updates are allowed.

The QRadar Console is responsible for downloading and providing updates to managed hosts in your deployment. You only need to complete this procedure on your Console.

Procedure

Step 1 Open your web browser.

Step 2 Log in to QRadar:

`https://<IP Address>`

Username: **`admin`**

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

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

Step 3 Click **Login To QRadar**.

A default license key provides you access to QRadar for five weeks. For more information about updating your license key, see the *IBM Security QRadar Administration Guide*.

Step 4 Click the **Admin** tab.

Step 5 On the navigation menu, click **System Configuration**.

Step 6 Click the **Auto Update** icon.

Step 7 On the navigation menu, click **Change Settings**.

Step 8 From the **Major Updates** list box, select **Disable**.

Step 9 From the **Minor Updates** list box, select **Disable**.

Step 10 Click **Save**.

The installation process is complete. You are now ready to use your QRadar appliance with FIPS enabled.

3 FIPS SHELL COMMANDS

You can use SSH to connect to an IBM Security QRadar FIPS appliance as the crypto or admin user with special account permissions.

Using crypto account shell commands

You can use crypto user accounts and the commands that are applied to this account to perform administrative tasks and maintain FIPS appliances.

Note: The crypto user account should be provided to security officers in your organization, as a crypto user can disable FIPS mode on a QRadar appliance.

Crypto are special user accounts that can enable FIPS mode, verify FIPS status on an appliance, or disable FIPS mode using shell commands. Crypto users are also allowed all of the commands provided to admin users for QRadar maintenance.

Procedure

Step 1 Using SSH, log in to QRadar as the FIPS crypto user.

Username: **`crypto`**

Password: **`<password>`**

Step 2 Type one of the following admin commands:

Table 1-3 Supported FIPS crypto commands

Command	Description
commit	Type the **commit** command to apply any changes made to a system file of your FIPS enabled system. The commit command includes the following options: • **--list** - The list option displays any system files that have been changed by the crypto user. • **--changes <file>** - The changes option display a list of differences in the file made by an admin of a FIPS enabled appliance. • **--check** - The verify option allows you to verify the list of files that are permitted for changes. • **--allowed** - The allowed option displays a list of system files that are allowed changes by an administrator of a FIPS enabled appliance. • **--force** - The force option allows an administrator to force a file change for files on the allowed list. Files not on the allowed file list are skipped. • **--revert <file>** - The revert option discards changes made to a specified file.
deploy	Type **deploy** to start a full deploy on a FIPS enabled appliance. This command restarts services on your appliance. ***Note:*** *Event and flow collection is stopped until the deploy process completes.*
disable_fips	Type **disable_fips** to disable FIPS mode on an appliance. This process restarts a number of services and requires a reboot of the appliance.
fips_self_check	Type **fips_self_check** to display the status of the operating system, required RPM files, log settings, and FIPS mode in the command line.
get_logs	Type **get_logs** to collect system data for your FIPS appliance.
mod_log4j	Type **mod_log4j** to modify log sources using the command-line interface of a FIPS enabled appliance.
reboot	Type **reboot** to restart a FIPS enabled appliance.
service	Type **service <service name> <start | stop | restart>** to change the status of a service on your QRadar appliance. For a list of services that can be restarted by the crypto user, type **service --list**.
shell	Type **shell** to access a command-line shell for viewing and editing files.
shutdown	Type **shutdown** to power off a FIPS enabled appliance.
help	Type **help** or **help <command>** to display the help interface for a specific admin or crypto FIPS command. Where **<command>** is any Crypto user command in this table.

Table 1-3 Supported FIPS crypto commands (continued)

Command	Description
exit	Type **exit** to log out of the crypto user account.

Using admin account shell commands

You can use the admin user accounts and the shell commands in this section to perform administrative tasks and maintain appliances.

Note: The admin user role should only be provided to administrators required to perform maintenance on a FIPS appliance in your organization.

Admin user accounts cannot disable, verify FIPS mode, or enable FIPS. Admin users are provided a specific set of command-line interface options that can be used to maintain a FIPS enabled system.

Procedure

Step 1 Using SSH, log in to QRadar as the FIPS admin user.

Username: **`admin`**

Password: **`<password>`**

Step 2 Type one of the following admin commands:

Table 1-4 Supported FIPS admin commands

Command	Description
commit	Type the **commit** command to apply any changes made to the system files of your FIPS enabled system. The commit command includes the following options: • **--list** - The list option displays any system files that have been changed by the admin user. • **--changes <file>** - The changes option display a list of differences in the file made by an admin of a FIPS enabled appliance. • **--check** - The verify option allows the admin to verify the list of files that are permitted for changes. • **--allowed** - The allowed option displays a list of system files that are allowed changes by an administrator of a FIPS enabled appliance. • **--force** - The force option allows an administrator to force a file change for files on the allowed list. Files not on the allowed file list are skipped. • **--revert <file>** - The revert option discards changes made to a specified file.
deploy	Type **deploy** to start a full deploy on a FIPS enabled appliance.
get_logs	Type **get_logs** to collect system data for your FIPS appliance.

Table 1-4 Supported FIPS admin commands (continued)

Command	Description
mod_log4j	Type **mod_log4j** to modify log sources using the command-line interface of a FIPS enabled appliance.
reboot	Type **reboot** to restart a FIPS enabled appliance.
shell	Type **shell** to access a command-line shell for viewing and editing files.
shutdown	Type **shutdown** to power off a FIPS enabled appliance.
help	Type **help** to see a list of commands available to an admin user.
exit	Type **exit** to log out of the admin user account.

4 FIPS USE CASES

The following use cases provide instructions for common tasks a crypto or admin user be required to complete with FIPS enabled appliances.

FIPS self-check

You can use the command-line interface to verify that FIPS is enabled on your appliance.

Procedure

Step 1 Using SSH, log in to QRadar as the crypto user.

Username: **crypto**

Password: **<password>**

Step 2 Type **fips_self_check**.

The output displays the status of your FIPS appliance.

```
Verifying Operating System ... (OK)
Verifying installed RPMs:
- kernel ... (OK)
- dracut-fips ... (OK)
- libgcrypt... (OK)
- openssl ... (OK)
- nss ... (OK)
- fipscheck-lib ... (OK)
Verifying Ariel Log Hashing Setting ... (OK)
FIPS mode: ON
```

If any self-check tests display missing files or error messages, contact support.

Disabling FIPS

You can use the command-line interface and crypto user account to disable FIPS mode on a QRadar appliance.

FIPS mode must be disabled in the following order:

1. Managed hosts
2. QRadar Console

Procedure

Step 1 Using SSH, log in to the QRadar FIPS appliance as a crypto user.

Username: **`crypto`**

Password: **`<password>`**

Step 2 Type the following command:

`disable_fips`

Step 3 Type **Yes** to disable FIPS mode.

Step 4 Type **reboot** to restart your QRadar appliance.

After the appliance restarts services, FIPS mode is disabled. You must repeat this process to disable FIPS mode on each additional appliance that is added to the Console as a managed host.

Restarting a service with FIPS enabled

You can use the following instructions to restart, stop, or start a service while FIPS is enabled.

Procedure

Step 1 Using SSH, log in to QRadar as the FIPS crypto user.

Username: **`crypto`**

Password: **`<password>`**

Step 2 Type **service --list** for a list of available QRadar services.

Step 3 Type **service <service name> <start | stop | restart>**.

Where:

<service name> is the name of the service.

<start | stop | restart> is the service action.

For example,

`service tomcat restart`

Step 4 Type exit to log out of the shell command-line interface.

Editing a configuration file with FIPS enabled

You can use the following instructions to change the content of a configuration file while FIPS is enabled.

QRadar includes default application IDs, however, you can edit the application mapping file to ensure that traffic is appropriately classified in the QRadar user interface. Any additional entries that you add to the mapping file override the default application IDs. This use case is intended to show an admin how to edit a default application ID when FIPS is enabled.

Procedure

Step 1 Using SSH, log in to QRadar as the FIPS admin or crypto user.

Username: **`admin`**

Password: **`<password>`**

Step 2 Type **shell** to use a command-line shell.

Step 3 Type **edit <file name>** to start editing a system configuration file.

For example,

`edit /store/configservices/staging/globalconfig/apps.conf`

Step 4 Save your changes.

Step 5 Type **exit** to exit the command shell.

Step 6 Type **commit --changes <file name>** to view the changes that are made to your configuration file.

For example,

`changes /store/configservices/staging/globalconfig/apps.conf`

Step 7 Type **commit** to apply the configuration file changes to your FIPS enabled appliance.

The file is update on your FIPS appliance.

```
Committed changes for
/store/configservices/staging/globalconfig/apps.conf
```

The file update is complete.

Adding a managed host to a FIPS deployment

To add a new managed host to your FIPS deployment, you must disable FIPS in your deployment, add the managed host, and re-enable FIPS mode with the command-line interface.

Procedure

Step 1 Log in as the crypto user and disable FIPS mode on all appliances in your deployment.

```
disable_fips
```

You must disable FIPS mode in the following order:

- Managed hosts
- QRadar Console

Step 2 Log in to your QRadar Console user interface.

Username: **`admin`**

Password: **`<password>`**

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 the managed host you are adding.
- **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 this check box to use an existing static Network Address Translation (NAT) address for this managed host. For more information about NAT, see the *QRadar 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 at least QRadar 5.1.
- **Enable Compression** - Select the check box to enable data compression between two managed hosts, each managed host must be running at least QRadar 5.1.

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: 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.

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 the public IP address to communicate with 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 Console, select the Console of the NATed network.
  - If the managed host is not on the same subnet as the Console, select the managed host of the NATed network.

Note: For information about managing your NATed networks, see the *QRadar Administration Guide*.

Step 8 Click **Next**.

Step 9 Click **Finish**.

A system message informs you that the deployment editor is adding the managed host. When this process is complete, you are returned to the **Admin** tab.

Step 10 On the **Admin** tab menu, click **Deploy Changes**.

Step 11 Using SSH, log in to your QRadar appliances as the crypto user to enable FIPS mode.

Step 12 Type the following command to enable FIPS mode:

```
/opt/qradar/fips/setup/fips_setup.py --enable
```

You must enable FIPS mode in the following order:

- Managed hosts
- QRadar Console

Step 13 Type **Yes** to enable FIPS mode.

Step 14 Type a password for the crypto user account.

The password must contain at least one special character, such as a period, comma, $, !, %, ^, or *.

Step 15 Retype the crypto password to confirm.

Step 16 Type a password for the admin user role.

The password must contain at least one special character, such as a period, comma, $, !, %, ^, or *.

Step 17 Retype the admin password to confirm.

Step 18 Type **reboot** to restart your QRadar appliance.

After the appliance restarts services, FIPS mode is enabled. The configuration is complete.

A CHANGING NETWORK SETTINGS

You must access the command line from a local connection or have access to the hardware to change the IP address of a QRadar system.

Note: Remotely updating your network settings by using SSH is not allowed. You can use SSH to remotely enable or disable FIPS, but the instructions assume that the entire process takes place at the console keyboard.

Change the network settings on an All-in-One Console

You can change the network settings in your All-In-One Console with FIPS mode.

You must perform this procedure in the following order:

1. **Changing network settings**
2. **Enabling FIPS mode**

Changing network settings

To change the network settings on an All-in-One Console appliance.

Procedure

Step 1 Log in to the QRadar command-line interface from the console connection:

Username: **`crypto`**

Password: **`<password>`**

Step 2 Type the following command to disable FIPS mode:

`disable_fips`

CAUTION: *Disabling FIPS mode stops services on your QRadar FIPS appliance and requires you to restart your appliance. Event and flow data cannot be collected while services are restarted.*

Step 3 Type **Yes** to confirm that you want to disable FIPS mode on your appliance.

Disabling FIPS enables the root user account for QRadar. You must restart to complete the process.

Step 4 Type **reboot** and press Enter.

After the appliance starts, you can log in to the appliance with the root user account. The root user account is created during the appliance installation.

Step 5 Log in to QRadar from a console connection:

Username: **root**

Password: **<password>**

Step 6 Type the following command:

qchange_netsetup

Step 7 Type Y to change the network settings.

Step 8 Select an Internet Protocol version. Select **Next** and press Enter.

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

Step 9 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 10 Choose one of the following options:

- If you are using IPv4 as your Internet Protocol, go to **Step 13**.
- If you are using IPv6 as your Internet Protocol, go to **Step 11**.

Step 11 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 amount of time. Go to **Step 13**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 12**.

Step 12 To enter network information to use for IPv6:

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

b Select **Next** and press Enter.

Step 13 Configure the QRadar 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. The public IP address is a secondary address that is used to access the server, usually from a different network or the Internet. The Public IP address is often configured with Network Address Translation (NAT) services on your network or firewall settings on your 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 14 Select **Finish** and press Enter.

A series of messages are displayed as QRadar processes the requested changes. After the requested changes are processed, the QRadar system is automatically shutdown and rebooted.You are now ready to enable FIPS mode.

Enabling FIPS mode

Use the command-line interface to enable FIPS mode on your QRadar appliance.

When you enable FIPS mode on a QRadar appliance, administrative access is provided only to the admin role or crypto user role. These accounts are created when you enable FIPS mode for QRadar. SSH access is restricted to the admin and crypto user accounts. Enabling FIPS on QRadar guides you through the process of creating these accounts.

Procedure

Step 1 Log in to the QRadar command-line interface from a console connection:

Username: **`root`**

Password: **`<password>`**

Step 2 Type the following command:

`/opt/qradar/fips/setup/fips_setup.py --enable`

If any required cryptographic files are missing, the output alerts you to the missing files.

Step 3 Type **Yes** to enable FIPS mode.

Step 4 Type a password for the crypto user role.

The password must contain at least one special character, such as a period, comma, $, !, %, ^, or *.

Step 5 Retype the crypto password to confirm.

Step 6 Type a password for the admin user role.

The password must contain at least one special character, such as a period, comma, $, !, %, ^, or *.

Step 7 Retype the admin password to confirm.

Step 8 Type **reboot** to restart your QRadar appliance.

After the appliance restarts services, FIPS mode is enabled. You must repeat this process to enable FIPS mode on every managed host in your deployment. The QRadar Console is the final appliance that you enable in FIPS mode.

Change the network settings of a large deployment

This use case provides step-by-step instructions on changing the IP address for a single managed host in a large FIPS deployment.

To change the network settings in a multi-appliance deployment, you must disable FIPS mode for your entire deployment. Then you can remove the managed host from the deployment editor and change the network settings. After the network settings are updated, you can add the managed host or hosts to your deployment and enable FIPS mode.

You must perform this procedure in the following order:

1. **Disabling FIPS**
2. **Removing a managed host**
3. **Changing network settings**
4. **Adding a managed host**
5. **Enabling FIPS mode**

Note: This procedure requires you to use the deployment editor. For more information about using the deployment editor, see the *IBM Security QRadar Administration Guide*.

Disabling FIPS

You can use the command-line interface and crypto user account to disable FIPS mode on a QRadar appliance.

FIPS mode disables several features that can be required by administrators. For example, when FIPS mode is enabled, you cannot:

- Add a managed host
- Remove a managed host
- Apply a software patch
- Change the IP address of an appliance.

Procedure

Step 1 Log in to the QRadar command-line interface from a console connection:

Username: **`crypto`**

Password: **`<password>`**

Step 2 Type the following command to disable FIPS mode:

`disable_fips`

CAUTION: *Disabling FIPS mode stops services on your QRadar FIPS appliance and requires you to reboot your appliance. Event and flow data cannot be collected while services are restarted.*

Step 3 Type **Yes** to confirm that you want to disable FIPS mode on your appliance.

Disabling FIPS enables the root user account for QRadar. You must reboot to complete the process.

Step 4 Type **reboot** and press Enter.

After the appliance reboots, you can log in to the appliance using the root user account you created during the initial appliance install.

Removing a managed host

You must remove the managed host from your deployment that requires a new IP address.

Procedure

Step 1 Log in to QRadar:

`https://<IP Address>`

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

Username: **`admin`**

Password: **`<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**.

Step 6 Click **Save**.

Step 7 Close the deployment editor.

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

The changes are deployed.

Changing network settings

The command-line interface allows you to change the network settings of a managed host.

Procedure

Step 1 Log in to the QRadar command-line interface from a console connection:

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 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 processes the requested changes. After the requested changes are processed, the QRadar system is automatically shutdown and rebooted.

Adding a managed host

You can use the Deployment Editor to add the managed host with a new IP address to your QRadar Console.

Procedure

Step 1 Log in to QRadar:

`https://<IP Address>`

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

Username: **`admin`**

Password: `<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**.

The Add a new host wizard is displayed.

Step 6 Click **Next**.

The Enter the host's IP window is displayed.

Step 7 Enter values for the parameters:

- **Enter the IP of the server or appliance to add** - Type the IP address of the host that you want to add to your System View.
- **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, 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**.

Step 10 Re-assign all components to your non-Console managed host.

a In the QRadar deployment editor, click the **Event View** tab.

b Select the component that you want to re-assign to the managed host.

c From the menu, select **Actions > Assign**

Note: You can also right-click a component to access the Actions menu items.

The Assign Component wizard is displayed.

d From the **Select a host** list box, select the host that you want to re-assign to this component. Click **Next**.

e Click **Finish**.

Step 11 Close the deployment editor.

Step 12 Click **Deploy Changes**.

The changes are deployed. You are now ready to enable FIPS mode.

Enabling FIPS mode

Use the command-line interface to enable FIPS mode on your QRadar appliance.

When you enable FIPS mode on a QRadar appliance, administrative access is provided only to the admin role or crypto user role. These accounts are created when you enable FIPS mode for QRadar. SSH access is restricted to the admin and crypto user accounts. Enabling FIPS on QRadar guides you through the process of creating these accounts.

You must enable FIPS in the following order:

1. Managed hosts
2. QRadar Console

Procedure

Step 1 Log in to the QRadar command-line interface from a console connection:

Username: **`root`**

Password: **`<password>`**

Step 2 Type the following command:

`/opt/qradar/fips/setup/fips_setup.py --enable`

If any required cryptographic files are missing, the output alerts you to the missing files.

Step 3 Type **Yes** to enable FIPS mode.

Step 4 Type a password for the crypto user role.

The password must contain at least one special character, such as a period, comma, $, !, %, ^, or *.

Step 5 Retype the crypto password to confirm.

Step 6 Type a password for the admin user role.

The password must contain at least one special character, such as a period, comma, $, !, %, ^, or *.

Step 7 Retype the admin password to confirm.

Step 8 Type **reboot** to restart your QRadar appliance.

After the appliance restarts services, FIPS mode is enabled. You must repeat this process to enable FIPS mode on every managed host in your deployment. The QRadar Console is the final appliance that you enable in FIPS mode.

B 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 *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.

UNIX is a registered trademark of The Open Group in the United States and other countries.

INDEX