IBM Security QRadar
Version 7.1.0 (MR1)

Setting Up an Autoupdate Server for QRadar Technical Note

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 7.

CONTENTS

1 SETTING UP A QRADAR SIEM UPDATE SERVER

IBM Security QRadar SIEM uses system configuration files to provide useful characterizations of network data flows. Updates to the system configuration files, available on the Qmmunity website (https://qmmunity.q1labs.com/), include minor updates (such as Online Help or script updates), major updates (such as JAR file updates), or Device Service Module (DSM) updates. Updates also include threat, vulnerability, and geographic information from various security-related websites.The QRadar SIEM Console must be connected to the Internet to receive automatic updates.

If your deployment includes a QRadar SIEM Console that is unable to access the Internet or you want to manually manage updates to your system, you can set up a QRadar SIEM update server to manage the update process.

The autoupdate package includes all files necessary to manually set up an update server in addition to the necessary system configuration files for each update. After the initial setup, you only need to download and uncompress the most current autoupdate package to manually update your configuration. To receive notification of new updates, we recommend that you access Qmmunity and subscribe to the following page: **Software** > **Autoupdates**.

This technical note provides information on manually setting up your QRadar SIEM update server. Unless otherwise noted, all references to QRadar SIEM refer to QRadar SIEM, IBM Security QRadar Log Manager, and IBM Security QRadar Network Anomaly Detection.

This includes the following sections:

Configuring your Update Server

You can either configure an Apache server or your QRadar SIEM Console as your update server. Choose one of the following procedures:

Configuring the Apache Server

To set up the Apache server:

Step 1 Access your Apache server.

Step 2 Create an update directory named **`autoupdates/`**.

By default, the update directory is located in the web root directory of the Apache server. You can place the directory in another location if you configure QRadar SIEM accordingly. For more information, see the *IBM Security QRadar SIEM Administration Guide*.

Step 3 Optional. Create an Apache user account and password to be used by the update process.

Step 4 Download the autoupdate package from the Qmmunity website.

a Go the Qmmunity website

`https://qmmunity.q1labs.com/`

b Select **Software** > **Autoupdates**.

c Double-click the latest autoupdate package matching your QRadar SIEM version.

d Save the file on your Apache server in the autoupdates directory created in **Step 2**.

Step 5 On the Apache server, type the following command to uncompress the autoupdate package.

```
tar -zxf updatepackage-[timestamp].tgz
```

Step 6 Configure QRadar SIEM to accept updates:

a Click the **Admin** tab.

b On the navigation menu, click **System Configuration**.

c Click **Auto Update**.

d To direct the update process to the Apache server, configure the following parameters in the **Server Configuration** panel:

- **Webserver** - Type the address or directory path of the Apache server.

NOTE If the Apache server runs on non-standard ports, add **`:<portnumber>`** to the end of the address. For example, https://qmmunity.q1labs.com/:8080.

- **Directory** - Type the directory location you created in **Step 2**.
- **Proxy Information** - Optional. If proxy information is required to access the Apache server, configure the following parameters:
  - **Proxy Server** - Type the URL for the proxy server.
  - **Proxy Port** - Type the port for the proxy server.
  - **Proxy Username** - Type the necessary username for the proxy server. A username is only required if you are using an authenticated proxy.

- **Proxy Password** - Type the necessary password for the proxy server. A password is only required if you are using an authenticated proxy.

e Select the **Deploy changes** check box.

f Click **Save**.

g Using SSH, Log in to QRadar SIEM as the root user.

Username: **root**

Password: **<admin password>**

h To configure the username and password for the Apache server, type the following commands:

/opt/qradar/bin/UpdateConfs.pl -change_username <username>

/opt/qradar/bin/UpdateConfs.pl -change_password <password>

The username and password must match those created in **Step 3**.

i To test your update server, type the following command:

lynx https://<your update server>/<directory path to updates>/manifest_list

j Type the username and password created in **Step 3**.

The list of updates is displayed. If the list is not displayed, contact Customer Support.

Configuring Your QRadar SIEM Console as the Update Server

You can configure your QRadar SIEM Console as the update server.

To set up your QRadar SIEM Console as the update server:

Step 1 Log in to QRadar SIEM as the root user.

Username: **root**

Password: **<admin password>**

Step 2 Type the following command to create the autoupdate directory:

mkdir /opt/qradar/www/autoupdates/

Step 3 Download the autoupdate package from the Qmmunity website.

a Go the Qmmunity website

https://qmmunity.q1labs.com/

b Select **Software** > **Autoupdates**.

c Double-click the latest autoupdate file matching your QRadar SIEM version.

d Save the file on your QRadar SIEM Console in the autoupdates directory created in **Step 2**.

Step 4 On your QRadar SIEM Console, type the following command to uncompress the autoupdate package.

tar -zxf updatepackage-[timestamp].tgz

Step 5 Configure QRadar SIEM to accept updates:

- **a** Log in to the QRadar SIEM user interface.
- **b** Click the **Admin** tab.
- **c** On the navigation menu, click **System Configuration**.
- **d** Click the **Auto Update** icon.
- **e** In the Server Configuration pane, type **`https://localhost/`** in the **Webserver** field.
- **f** If the **Send feedback** option in the Update Settings pane is enabled, clear the check box to disable it.

Step 6 Click **Save and Update Now**.

Adding New Updates

After you have configured your update server and set up QRadar SIEM to receive updates from the update server, adding new updates only requires you to download updates from the Qmmunity website to your update server.

To add new updates to the server:

Step 7 Download the update file from the Qmmunity website.

- **a** Go the Qmmunity website

  `https://qmmunity.q1labs.com/`
- **b** Select **Software** > **Autoupdates**.
- **c** Double-click the latest autoupdate package matching your QRadar SIEM version.
- **d** Save the file on your local update server in the directory you created when setting up your update server.

Step 8 Access your update server.

Step 9 Type the following command to uncompress the autoupdate package.

`tar zxf <updatepackage.tgz>`

Step 10 Log in to QRadar SIEM as root.

Step 11 Test your update server, type the following command:

`lynx https://<your update server>/<directory path to updates>/manifest_list`

Step 12 Type the username and password of your update server.

The list of updates is displayed. If not, contact Customer Support.

A NOTICES AND TRADEMARKS

What's in this appendix:

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

Notices

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

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

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

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

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

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

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

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

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

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

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

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

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

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

capabilities of non-IBM products should be addressed to the suppliers of those products.

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

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

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

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

Trademarks

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