IBM Security QRadar
Version 7.1.0 (MR1)

Replacing the SSL Certificate Technical Note

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 5

CONTENTS

1 REPLACING THE SSL CERTIFICATE

By default, QRadar provides an untrusted SSL certificate. You can replace the untrusted SSL certificate with a self-signed or trusted certificate.

Unless otherwise noted, all references to QRadar SIEM refer to QRadar SIEM, QRadar SIEM Log Manager, and QRadar SIEM Network Anomaly Detection.

This document includes the following topics:

Understanding SSL Certificates

Secure Sockets Layer (SSL) is the transaction security protocol used by websites to provide an encrypted link between a web server and a browser. SSL is an industry standard and is used by websites to protect online transactions. To be able to generate an SSL link, a web server requires an SSL certificate. SSL certificates are issued by:

- **Software** - Generally available software, such as Open SSL or Microsoft's Certificate Services manager, issues SSL certificates. These certificates are not inherently trusted by browsers, because they are not issued by a recognized authority. Although they can be used for encrypting data, there is no third-party assurance regarding the identity of the server sending the certificate. They cause browsers to display warning messages that inform the user that the certificate has not been issued by an entity that the user has chosen to trust.
- **Trusted third-party certifying authorities** - These certification authorities, such as VeriSign or Thawte, use their trusted position to issue trusted SSL certificates. SSL certificates issued by trusted certification authorities do not display a warning and transparently establish a secure link between a website and a browser.

Browsers and operating systems include a pre-installed list of trusted certification authorities, known as the Trusted Root CA (Certificate Authority) store. As Microsoft and Mozilla provide the major operating systems and browsers, they elect whether or not to include the certification authority into the Trusted Root CA store, thereby giving the certification authority its trusted status. Java™ Runtime

Environment provides a set of trusted certificated authorities, as selected by Sun Microsystems.

For the purpose of establishing SSL connections between the browser and Console, QRadar trusts any certificate that is issued, directly or indirectly, from a trusted root CA in the browser and Java™ keystore.

For the purpose of establishing all internal SSL connections between components, QRadar does not trust certificates issued by a recognized authority. Instead, you must use the web server certificate pre-installed on the Console.

Replacing the Default SSL Certificate

You can replace the untrusted SSL certificate with either a self-signed certificate or a certificate issued by a trusted third-party certifying authority.

CAUTION

We recommend that you do not encrypt the private key when installing or replacing an SSL certificate. If you encrypt the private key, your Console system pauses until you manually enter a password each time the Console restarts. This delay can disrupt event collection.

To replace the SSL certificate on your QRadar SIEM Console:

Step 1 Obtain a certificate from a trusted certificate authority.

NOTE

SSL certificates issued from some vendors, such as VeriSign, require an intermediate certificate. You must download the intermediate certificate from the vendor and use it during the configuration.

Step 2 Using SSH, log in to your QRadar SIEM Console as the root user:

Username: **root**

Password: **<password>**

Step 3 Choose one of the following options:

- If you require an intermediate certificate, see **Step 4**.
- If you do not require an intermediate certificate, see **Step 5**.

Step 4 If you require an intermediate certificate, follow this procedure:

a Type the following command:

```
/opt/qradar/bin/install_ssl_cert.sh -i
```

The following message and prompt are displayed:

```
This script installs a new SSL certificate
Path to private key file (SSLCertificateKeyFile):
```

b Type the directory path for your private key file. Press Enter on your keyboard.

The following prompt is displayed:

```
Path to public key file (SSLCertificateFile):
```

c Type the directory path for your public key file. Press Enter on your keyboard.

The following prompt is displayed:

```
Path to SSL intermediate certificate file
(SSLCACertificateFile - optional):
```

d Type the directory path for your intermediate certificate. Press Enter on your keyboard.

The following messages and prompt are displayed:

```
You have specified the following:
SSLCertificateKeyFile of '<private certificate directory
path>'
SSLCertificateFile of '<public certificate directory path>'
SSLCACertificateFile of '<intermediate certificate directory
path>'

Continue and reconfigure Apache now (includes restart of httpd
daemon) (Y/[N])?
```

e Type **Y** to continue. Press Enter on your keyboard.

The following messages are displayed:

```
Changing the SSL certificate configuration variable ...
Restarting Apache
Stopping httpd: [ OK ]
Starting httpd: [ OK ]
Restarting HostContext
[Q] Shutting down hostcontext service: [ OK ]
[Q] Starting hostcontext service: [ OK ]
Successfully done.
```

Go to **Step 6**.

Step 5 If you do not require an intermediate certificate, follow this procedure:

a Type the following command:

```
/opt/qradar/bin/install_ssl_cert.sh -b
```

The following messages and prompt are displayed:

```
This script installs a new SSL certificate

Path to private key file (SSLCertificateKeyFile):
```

b At the **Path to private key file** prompt, type the directory path for your private key file. Press Enter on your keyboard.

The following prompt is displayed:

```
Path to public key file (SSLCertificateFile):
```

c Type the directory path for your public key file. Press Enter on your keyboard.

The following messages and prompt are displayed:

```
You have specified the following:
SSLCertificateKeyFile of '<private certificate directory
path>'
SSLCertificateFile of '<public certificate directory path>'

Continue and reconfigure Apache now (includes restart of httpd
daemon) (Y/[N])?
```

d Type **Y** to continue. Press Enter on your keyboard.

The following messages are displayed:

```
Changing the SSL certificate configuration variable ...
Restarting Apache
Stopping httpd: [ OK ]
Starting httpd: [ OK ]
Restarting HostContext
[Q] Shutting down hostcontext service: [ OK ]
[Q] Starting hostcontext service: [ OK ]
Successfully done.
```

Step 6 Type the following command to restart the host context process on all non-Console systems in your deployment:

```
service hostcontext restart
```

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*.

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

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

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