Product Verification Checklist

for RSA NetWitness ® Platform v11.7

Copyright © 2022 RSA Security LLC or its subsidiaries. All Rights Reserved.

December 2022

Trademarks

RSA and the RSA Logo are either registered trademarks or trademarks of RSA in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks

License Agreement

This software and the associated documentation are proprietary and confidential to RSA, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the thirdpartylicenses.pdf file.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA software described in this publication requires an applicable software license. RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Contents

Product Validation Checklist 3

Hardware Validation 3

Software Validation 4

Product Validation Checklist

This checklist provides procedures for validating that the hardware and software products that you receive are the ones that you purchased from RSA.

Hardware Validation

Before you open the packaging of the hardware, ensure that the box in which the hardware arrives is not damaged or previously opened, and has not been tampered with. Verify the following:

The package is not dented or broken.

All labels are sealed and unbroken.

There is no text on the package that says “OPENED.”

When you open the package, inspect the hardware. Verify the following:

The hardware that was shipped is the version that you ordered. When you first boot the system, the version number of the product displays in the start process.

The appliance serial number on the hardware matches the appliance serial number on the RSA packing slip. The following is an example of where the serial number is displayed on the RSA packing slip:

RSA Model #	RSA Description For Labels	Dell Reg. No	Serial Number
NW-S6H-AS	NW S6 Analytics Server	E39S	3KDMYR2

Software Validation

NOTE: The Common Criteria evaluation is based on RSA NetWitness 11.7.1.2. The end user needs to download the 11.7.0.0 OVA or ISO from my.rsa.com and then update the stack to 11.7.1.2.

All product software is included in the OVA download. A VM instance can be created out of the OVA download

Validate the checksum of each OVA file for the product that you purchased, and compare it to the checksum of the OVA file from the download site to be sure that the checksum files match.

1. On a Windows system, verify the checksum by running the `CertUtil` command:

   At a command line prompt, in the folder where the OVA files are installed, run the following command:

   ```
   CertUtil -hashfile pathToFileToCheck <HashAlgorithm>
   ```

   Applicable examples of hash algorithms are:

   ```
   MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512
   ```

   For example, on the RSA-NW OVA system, you can find the MD5 hash by running the following command:

   ```
   certutil -hashfile rsa-nw-11.7.0.0.17934-x86_64.ova MD5
   ```

   which results in output similar to the following:

   ```
   MD5 hash of rsa-nw-11.7.0.0.17934-x86_64.ova:
    3fc3be89e5e03784d15800c41713a2ba
    CertUtil: -hashfile command completed successfully.
   ```

2. On a Unix system, verify the checksum by running either the `md5sum` or `sha (sha1, sha256, sha512)` command. In the folder where the OVA files are installed, run the following command:

   ```
   md5sum pathToFileToCheck
   ```

   For example, on the RSA-NW OVA system, you can find the MD5 hash by running the following command:

md5sum rsa-nw-11.7.0.0.17934-x86_64.ova which results in output similar to the following: 3fc3be89e5e03784d15800c41713a2ba

rsa-nw-11.7.0.0.17934-x86_64.ova and you would ensure that 3fc3be89e5e03784d15800c41713a2ba matches the checksum provided on the download site.