



NetWitness® Endpoint 4.4.1.1 Release Notes

for Version 4.4.1.1



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

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 on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

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

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

August 2019

Contents

Introduction	4
Update Notes	4
Product Documentation	5
Fixed Issues	6
Known Issues	7
Installation	9
Installation Prerequisites	10
RAID Configuration	10
Database Backup	10
Microsoft Windows Update Service	10
Installation Procedure	11
Contacting Customer Care	13
Revision History	14

Introduction

This document describes the enhancements and fixes included in RSA NetWitness® Endpoint 4.4.1.1. RSA recommends reading this document before installing and using RSA NetWitness Endpoint 4.4.1.1. This document contains the following sections:

- [Update Notes](#)
- [Product Documentation](#)
- [Fixed Issues](#)
- [Known Issues](#)
- [Installation](#)
- [Contacting Customer Care](#)
- [Revision History](#)

Update Notes

You cannot install version 4.4.1.1 as a new release. You must update to this version from an existing installation of the product. RSA NetWitness Endpoint 4.4.1.1 supports upgrade paths from previous versions, as follows:

- The following RSA NetWitness Endpoint releases may update directly to RSA NetWitness Endpoint 4.4.1.1:
 - RSA NetWitness Endpoint 4.4.0.8
 - RSA NetWitness Endpoint 4.4.0.9
 - RSA NetWitness Endpoint 4.4.1.0
- Users on all other versions must first upgrade to a supported version before updating to 4.4.1.1.
- If you are installing RSA NetWitness Endpoint for the first time, you must install version 4.4.0.0, upgrade to version 4.4.1.0, and then update to version 4.4.1.1.

Note: To upgrade to version 4.4.1.1 from version 4.3.x, you must first upgrade to version 4.3.0.6, and then upgrade to version 4.4.0.8. You can then upgrade from version 4.4.0.8 to 4.4.1.1.

Note: If you have configured your previous version of NetWitness Endpoint to work with OPSWAT Metascan (now called Metadefender Core) v3, once you update to NetWitness Endpoint 4.4.0.1 or later, you must download and install OPSWAT Metadefender Core v4.8.0. OPSWAT Metadefender v3 will not work with NetWitness Endpoint 4.4.0.1 or later. For directions on downloading and installing OPSWAT Metadefender Core, see the topic "Step 9: (Optional) Install Metascan" in the latest version of the *NetWitness Endpoint 4.4 Installation Guide*.

Note: For all agents communicating through the Roaming Agents Relay (RAR), you should wait until agents are communicating directly to the ConsoleServer before updating to ensure a successful update.

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA NetWitness Endpoint 4.4 User Guide	https://community.rsa.com/docs/DOC-81665
RSA NetWitness Endpoint 4.4 Installation Guide	https://community.rsa.com/docs/DOC-81664

Fixed Issues

This section lists issues that were found in RSA NetWitness Endpoint 4.4.0.x and fixed in RSA NetWitness Endpoint 4.4.1.1.

Note: The fixed issues only refer to issues fixed in this release. To check issues fixed in releases previous to 4.4.1.1, refer the respective release notes, available on [RSA Link](#).

Issue #	Description
ECATCE-1226	Unknown kernel encodings on Windows Server 2008, build 6003.
ECATCE-1221	Issues integrating ECAT 4.4.0.6 with RSA Netwitness 11.3 for Message Bus.
ECATCE-1220	Triggered IOC did not send an alert to remote SIEM tool.
ECATCE-1216	The User Interface is not showing all tracking events.
ECATCE-1209	LaunchArguments table grows too large.
ECATCE-1205	nwe-agent service on CentOS 7 crashes.
ECATCE-1202	IOC evaluation incorrectly triggered on whitelisted modules, causing user confusion with missing alerts.
ECAT-8948	LiveFeedback authentication failure can produce the wrong error message.
ECAT-8947	Unsigned IOCs are triggering on a signed module.
ECAT-8946	Agent does not report an error to the server when the kernel update command fails.

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it is noted or referenced in detail.

Tracking Number: ECATCE-1026

Problem: The user interface for the Machines, Modules, and Certificates views is out of sync with database tables.

Workaround: Click **Shift-F5** to clear the cache and to reload the list from the database.

Tracking Number: ECATCE-995

Problem: The Windows 10 Device Guard feature is not supported in NetWitness Endpoint 4.4.x agents.

Workaround: None

Tracking Number: ECATCE-822

Problem: When doing a fresh install of NetWitness Endpoint 4.4.x, if the "sa" sysadmin account was previously removed from the MSSQL database, a database error occurs.

Workaround: Enable or recreate the "sa" sysadmin account for the MSSQL database and repeat the NetWitness Endpoint installation process.

Tracking Number: ECATCE-763

Problem: In the Modules view, when a user right-clicks a column header and selects Column Chooser, if the user expands the Reputation category in the Customization dialog, the user is unable to scroll to the last item, which is Yara Scan result.

Workaround: In the UI, use the search area to find "Yara scan result."

Tracking Number: ECAT-8741

Problem: If a user applies a filter to the Machine View, changes the column order, then closes and restarts the NetWitness Endpoint UI, the Machine View display is blank and the following error message is displayed: "Error occurred during processing server request (The binary operator Equal is not defined for the...)." This occurs because the grid view layout for the Machine view, including the column order and filter, is saved to disk when column order is changed by the user. When the UI is restarted, the previous filter and the previous column order are both reapplied.

Workaround: To prevent this issue, user should avoid applying filters to the Machine View when also making any column modifications, such as reordering or adding or removing. To recover from this issue, the user should remove the applied filter and do some reordering of columns, which will overwrite the previously saved filter on disk. The user can then continue to work as usual.

Tracking Number: ECAT-8349

Problem: In the Machine and Module views, the row count shows as "0" for a group even though the group has rows.

Workaround: The user can expand each group to update the group count data.

Tracking Number: ECAT-8301

Problem: If a NetWitness Endpoint user has subscribed to RSA Live feeds, when that user upgrades to a newer version, all the subscribed feeds get cleared.

Workaround: After upgrading NetWitness Endpoint, in the NetWitness Endpoint UI, navigate to **Configure > External Components Configuration**. On the External Components Configuration dialog, select to edit the RSA Live configuration. On the RSA Live dialog, click **Select All** and then click **Save**.

Tracking Number: ECAT-7884

Problem: If you decommission a server with an agent under containment, the agent will be moved to the Primary server. However, after this point, the agent will be self-contained, because it does not have the Primary server IP in the exclusion list.

Workaround: You must manually reinstall a new agent on the machine.

Tracking Number: ECAT-7545

Problem: Mac IIOC alertable value set to False after upgrade of ConsoleServer.

Workaround: Manually change Mac IIOC alertable values to True after the upgrade.

Tracking Number: ECAT-7263

Problem: Updating of agents while in Roaming Agents Relay (RAR) mode is not supported.

Workaround: Update agent only when agent is communicating directly to the ConsoleServer.

Tracking Number: ECAT-7213/ECAT-7214

Problem: The Delete from Quarantine function was not working correctly and was removed from the RSA NetWitness Endpoint UI.

Workaround: Do not use any quarantine features.

Installation

You cannot install version 4.4.1.1 as a new release. You must update to this version from an existing installation of the product. RSA NetWitness® Endpoint 4.4.1.1 supports upgrade paths from previous versions, as follows:

- The following RSA NetWitness Endpoint releases may update directly to RSA NetWitness Endpoint 4.4.1.1:
 - RSA NetWitness Endpoint 4.4.0.8
 - RSA NetWitness Endpoint 4.4.0.9
 - RSA NetWitness Endpoint 4.4.1.0
- Users on all other versions must first upgrade to a supported version before updating to 4.4.1.1.
- If you are installing RSA NetWitness Endpoint for the first time, you must install version 4.4.0.0, upgrade to version 4.4.1.0, and then update to version 4.4.1.1

Note: To upgrade to version 4.4.1.1 from version 4.3.x, you must first upgrade to version 4.3.0.6, and then upgrade to version 4.4.0.8. You can then upgrade from version 4.4.0.8 to 4.4.1.1.

Note: If you have modified the `metakeysconfiguration.xml` file (default location: `C:\Program Files\RSA\ECAT\Server`), you must make a backup copy of this file before updating to a later version of NetWitness Endpoint 4.4. After the update is complete, you will need to manually restore the mappings from the backup configuration file.

Note: It is considered a best practice for RSA NetWitness Endpoint agents to be updated to the installed version. If merge issues are encountered, agents need to be updated to RSA NetWitness Endpoint 4.4.1.1.

Note: NetWitness Endpoint agents can upgrade from any lower version to a higher version of NetWitness Endpoint, as long as the NetWitness Endpoint Console Server version is either higher than or equal to the agent version.

Note: If you have configured your previous version of NetWitness Endpoint to work with OPSWAT Metascan (now called Metadefender Core) v3, once you update to NetWitness Endpoint 4.4.0.1 or later, you must download and install OPSWAT Metadefender Core v4.8.0. OPSWAT Metadefender v3 will not work with NetWitness Endpoint 4.4.0.1 or later. For directions on downloading and installing OPSWAT Metadefender Core, see the topic "Step 9: (Optional) Install Metascan" in the latest version of the *NetWitness Endpoint 4.4 Installation Guide*.

Note: For all agents communicating through RAR, you should wait until agents are communicating directly to the ConsoleServer before updating to ensure a successful update.

Note: The installation directory for Linux agents changed with release 4.3.0.4. The new installation directory for Linux agents 4.3.0.4 and higher is: `/opt/rsa/nwe-agent`. Additionally, the agent binary is located in `/opt/rsa/nwe-agent/bin`. The certificate and configuration files are located in `/opt/rsa/nwe-agent/config`. The service name has also changed from `ecat-agent` to `nwe-agent`. To stop or start the agent, you need to execute the service `nwe-agent stop` or `service nwe-agent start` command, respectively. To uninstall the agent, execute `rpm -e nwe-agent` command.

Installation Prerequisites

RAID Configuration

RSA strongly recommends the following configuration when using a single RAID 10 volume for the RSA NetWitness Endpoint Microsoft SQL database: You must use a 64K block size in Windows with a 1024 offset and NTFS file system when formatting the partition. If this is not the configuration used, there could be serious impacts to system performance.

Database Backup

It is also strongly recommended to backup all RSA NetWitness Endpoint Microsoft SQL databases, primary and secondary, and create a backup copy of the server and client certificates. For complete details, see the "Update Installation" section of the *RSA NetWitness Endpoint 4.4.x Installation Guide*.

Note: Supported versions of Microsoft SQL Server are: MSSQL 2012, MSSQL 2014, and MSSQL 2016 Standard and Enterprise Editions.

Microsoft Windows Update Service

To avoid a potential error message during the RSA NetWitness Endpoint update procedure, caused by the Microsoft Windows Update service affecting the connection to the MSSQL Server, it is strongly recommended that you stop the Windows Update service before initiating the RSA NetWitness Endpoint update installation. Furthermore, to avoid interference with the RSA NetWitness Endpoint system, RSA recommends that you keep the Windows Update service turned off and use the following process for applying Windows Updates:

1. Stop the RSA ECAT Server and RSA ECAT API Server services.
2. Stop the SQLServerAgent service.
3. Turn on the Windows Update service and proceed with the Windows Update and all necessary steps such as download, installation, and reboot.
4. When the Windows Update is complete, turn off the Windows Update service.
5. Restart the SQLServerAgent service.
6. Restart the ECAT Server and ECAT API Server services.

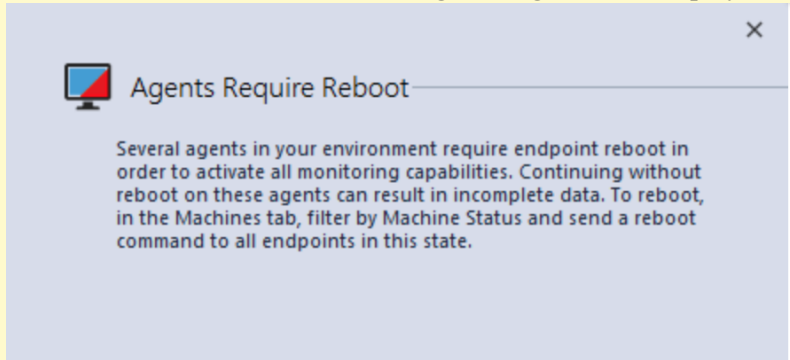
Installation Procedure

To update from a supported update version of RSA NetWitness Endpoint, see the complete update instructions in the "Update Installation" section of the *RSA NetWitness Endpoint 4.4 Installation Guide*, using the 4.4.1.1 archive file (**rsa_nwe_4.4.1.1_sw.zip**).

If you are currently using the Roaming Agents Relay (RAR), you will also need to update RAR to version 4.4.1.1, as described in the "Update Installation" section of the *RSA NetWitness Endpoint 4.4 Installation Guide*, using the 4.4.1.1 archive file (**rsa_nwe_4.4.1.1_roaming_agents_relay.zip**).

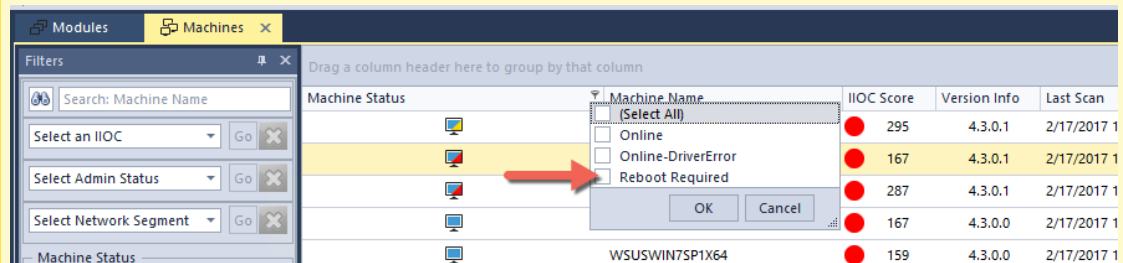
Note: NetWitness Endpoint 4.4.1.1 release does not support full install of the product.

Caution: After updating agents to 4.4, when the Machines table is loaded in the RSA NetWitness Endpoint UI, if any RSA NetWitness Endpoint agents are currently in the driver error 0x20010007 state, the following message will be displayed:



You must reboot the affected machines to ensure agents are collecting complete data, as follows:

1. In the Machines table, select to filter the Machine Status column by **Reboot Required**, as shown below:



2. Select all machines that match that status (these machines will all have this machine status icon: .)

3. Right-click and select **Advanced > Reboot...**

For more information on rebooting machines, see the "Reboot a Machine" topic in the *RSA NetWitness® Endpoint 4.4 User Guide*.

Note: Beginning with RSA NetWitness Endpoint 4.3.0.1, encryption for generated certificates has changed from SHA1 to SHA256 and the length has also changed from 2048 to 4096. This change will not be apparent to users. However, if users elect to generate new certificates, the certificate names will change as follows: EcatCA is now NweCA, EcatClientExported is now NweAgentCertificate, and EcatServerExported is now NweServerCertificate. You can also still select to continue using existing certificates, in which case the certificate names will not change, but will continue to be valid.

Contacting Customer Care

When you contact Customer Care, you should be at your computer. Be prepared to give the following information:

- The version number of the RSA NetWitness Endpoint product or application you are using.
- The type of hardware you are using.

Use the contact information provided at the following location if you have any questions or need assistance: <https://community.rsa.com/docs/DOC-1294>.

Revision History

Revision	Date	Description
01	Sept 2019	Final version