



Release Notes

for Version 11.2.1



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 EMC, 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 EMC.

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

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

Contents

Introduction	4
What's New	4
NetWitness User and Entity Behavior Analysis (UEBA)	4
Fixed Issues	4
Security	4
Server	5
Reporting	5
Investigate	5
Health and Wellness	6
Event Stream Analysis	6
Core Services	6
Build Numbers	6
Update Notes	7
Known Issues	8
UEBA	8
Product Documentation	8
Feedback on Product Documentation	9
Contacting Customer Care	9
Revision History	9

Introduction

This document lists enhancements and fixes in NetWitness Platform 11.2.1.0. Read this document before deploying or updating to NetWitness Platform 11.2.1.0.

What's New

The NetWitness Platform 11.2.1.0 release provides the following enhancement.

NetWitness User and Entity Behavior Analysis (UEBA)

Support for Remote Access Model. UEBA now models user access to remote computers using the Remote Desktop Protocol. This model defines each user's commonly accessed remote computers and flags any abnormal access. For more information, see *RSA NetWitness UEBA User Guide*.

Fixed Issues

This section lists issues fixed since the last major release.

Security

Tracking Number	Description
ASOC-61704	Yum-utils Security Update https://access.redhat.com/errata/RHSA-2018:2285
ASOC-61929	Kernel Security Update https://access.redhat.com/errata/RHSA-2018:2384
ASOC-59638	Gnupg2 Security Update https://access.redhat.com/errata/RHSA-2018:2181
ASOC-62742	postgresql Security Update https://access.redhat.com/errata/RHSA-2018:2557
ASOC-62744	Bind Security Update https://access.redhat.com/errata/RHSA-2018:2570

Tracking Number	Description
ASOC-59640	Python Security Update https://access.redhat.com/errata/RHSA-2018:2123
ASOC-66836	Openjdk Security Update https://access.redhat.com/errata/RHSA-2018:2942
ASOC-63750	Upgrade Erlang library to version 20.3 to mitigate ROBOT attack on TLS vulnerability

Server

Tracking Number	Description
SACE-10385/ SACE-10364	Health and Wellness view does not display the options to view updated pages.
SACE-9850	In the Charts view, when you sort on a column, the results are not displayed.

Reporting

Tracking Number	Description
SACE-10456	In the Rules view, when defining a WHERE clause, additional space is automatically added after each condition.

Investigate

Tracking Number	Description
SACE-10329	When you query on the Investigation view, you cannot enter special characters in the query dialog.
SACE-10162	Investigation query with meta groups do not support IP addresses in the CIDR format.

Tracking Number	Description
SACE-10060	Metakeys with integer type displays IntelliSense error when you select the options from Operators drop-down.

Health and Wellness

Tracking Number	Description
SACE-10237	When you export event sources, an invalid CSV file is created.

Event Stream Analysis

Tracking Number	Description
SACE-9793	An error occurs when Whois service is configured.

Core Services

Core Services include Broker, Concentrator, Decoder, and Log Decoder.

Tracking Number	Description
SACE-10222	Logs are missing in the output file when the Concentrator is restarted.

Build Numbers

The following table lists the build numbers for various components of NetWitness Platform 11.2.1.0.

Component	Version Number
NetWitness Platform Decoder	11.2.1.0 - 9484.5
NetWitness Platform Concentrator	11.2.1.0 - 9484.5
NetWitness Platform Broker	11.2.1.0 - 9484.5

NetWitness Platform Log Decoder	11.2.1.0 - 9484.5
NetWitness Platform Archiver (Workbench)	11.2.1.0 - 9484.5
NetWitness Platform Event Stream Analysis Server	11.2.1.0 - 79.5
NetWitness Platform Appliance	11.2.1.0 - 9484.5
NetWitness Platform Archiver	11.2.1.0 - 9484.5
NetWitness Platform Cloud Gateway Server	11.2.1.0 - 181227095924.5
NetWitness Platform Console	11.2.1.0 - 9484.5
NetWitness Platform Endpoint Agents	11.2.1.0 - 1901021449.5
NetWitness Platform Endpoint Server	11.2.1.0 - 181227054005.5
NetWitness Platform Investigate Server	11.2.1.0 - 181227054240.5
NetWitness Platform Malware Analysis Server	11.2.1.0 - 190121122402.5
NetWitness Platform Legacy Web Server	11.2.1.0 - 190121135008.5
NetWitness Platform Log Player	11.2.1.0 - 9484.5
NetWitness Platform Orchestration Server	11.2.1.0 - 181227054452.5
NetWitness Platform Respond Server	11.2.1.0 - 181227053905.5
NetWitness Platform SDK	11.2.1.0 - 9484.5
NetWitness Platform Security Server	11.2.1.0 - 181227054515.5

Update Notes

The following update paths are supported for NetWitness Platform 11.2.1.0:

- RSA NetWitness® Platform 11.1.0.0 to 11.2.1.0
- RSA NetWitness® Platform 11.1.0.1 to 11.2.1.0
- RSA NetWitness® Platform 11.1.0.2 to 11.2.1.0
- RSA NetWitness® Platform 11.1.0.3 to 11.2.1.0

- RSA NetWitness® Platform 11.2.0.0 to 11.2.1.0
- RSA NetWitness® Platform 11.2.0.1 to 11.2.1.0

For more information on updating to 11.2.1.0, see the [Update Instructions](#) section.

Known Issues

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

UEBA

UEBA Service displays incorrect version.

Tracking Number: ASOC-69605

Problem: After you update NetWitness Platform to 11.2.1, the **ADMIN > Hosts** view displays incorrect UEBA version.

Workaround: You need to update the UEBA service.

1. Go to **ADMIN > Hosts**.
2. Select the UEBA host.
3. Click **Update > Update Host** from the toolbar.
4. Click **Begin Update**.

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
RSA NetWitness Platform 11.2 Online Documentation	https://community.rsa.com/community/products/netwitness/112
RSA NetWitness Platform 11.2 Upgrade Instructions	RSA NetWitness Platform 11.2 Upgrade Instructions
RSA NetWitness Platform 11.2.1.0 Update Guide	https://community.rsa.com/docs/DOC-100370

Feedback on Product Documentation

You can send an email to sahelpfeedback@emc.com to provide feedback on RSA NetWitness Platform documentation.

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 Platform product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

RSA Link	https://community.rsa.com In the main menu, click My Cases .
Phone	1-800-995-5095, option 3
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Community	https://community.rsa.com/community/support
Basic Support	Technical Support for your technical issues is available from 8 AM to 5 PM your local time, Monday through Friday.
Enhanced Support	Technical Support is available by phone 24 x 7 x 365 for Severity 1 and Severity 2 issues only.

Revision History

Revision	Date	Description
1.0	25-Jan-19	Final Draft