



# Release Notes

for RSA NetWitness Platform 11.1.0.3



## **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](http://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. By using this product, a user of this product agrees to be fully bound by terms of the license agreements applicable to third-party software in this product.

## **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.

July 2019

# Contents

---

<b>Introduction</b> .....	<b>4</b>
<b>Build Numbers</b> .....	<b>5</b>
<b>Update Instructions</b> .....	<b>6</b>
Update Tasks .....	6
Online Method (Connectivity to Live Services): Update Using NetWitness User Interface .....	6
Prerequisites .....	6
Procedure .....	7
Offline Method (No connectivity to Live Services): Update using the Command Line Interface .....	8
Prerequisites .....	8
Procedure .....	8
External Repo Instructions for CLI Update .....	9
Post-Update Tasks .....	10
Task 1 (Optional) - Move the custom certs .....	10
Task 2 (Conditional) - Reconfigure PAM Radius Authentication .....	10
Task 3 - Restart the Respond Server .....	11
<b>Fixed Issues</b> .....	<b>12</b>
Security Fixes .....	12
Server Fixes .....	12
Investigate Fixes .....	12
Core Fixes .....	12
<b>Known Issues</b> .....	<b>14</b>
Server .....	14
Respond .....	14
<b>Product Documentation</b> .....	<b>15</b>
<b>Contacting Customer Care</b> .....	<b>16</b>
Preparing to Contact Customer Care .....	16
<b>Revision History</b> .....	<b>17</b>

## Introduction

---

This document lists fixes in RSA NetWitness Platform 11.1.0.3. Read this document before deploying or updating RSA NetWitness Platform 11.1.0.3.

- [Build Numbers](#)
- [Update Instructions](#)
- [Fixed Issues](#)
- [Known Issues](#)
- [Product Documentation](#)
- [Contacting Customer Care](#)
- [Revision History](#)

## Build Numbers

The following table lists the build numbers for various components of RSA NetWitness Platform 11.1.0.3.

Component	Version Number
Netwitness Suite Web Server	11.1.0.3-180912012335.5
Netwitness Suite Decoder	11.1.0.3-9078.5
Netwitness Suite Concentrator	11.1.0.3-9078.5
Netwitness Suite Broker	11.1.0.3-9078.5
Netwitness Suite Log Decoder	11.1.0.3-9078.5
Netwitness Suite Archiver (Workbench)	11.1.0.3-9078.5
Netwitness Suite Event Stream Analysis Server	11.1.0.3-10.5
Netwitness Suite Appliance	11.1.0.3-9078.5
Netwitness Suite Archiver	11.1.0.3-9078.5
Netwitness Suite Cloud Gateway Server	11.1.0.3-180912012409.5
Netwitness Suite Concentrator	11.1.0.3-9078.5
Netwitness Suite Console	11.1.0.3-9078.5
Netwitness Suite Endpoint Server	11.1.0.3-180912012727.5
Netwitness Suite Investigate Server	11.1.0.3-180912012959.5
Netwitness Suite Legacy Web Server	11.1.0.3-180912095327.5
Netwitness Suite Log Player	11.1.0.3-9078.5
Netwitness Suite Respond Server	11.1.0.3-180912013210.5
Netwitness Suite SDK	11.1.0.3-9078.5

## Update Instructions

---

You need to read the information and follow these procedures for updating RSA NetWitness Platform version 11.1.0.3.

The following update paths are supported for RSA NetWitness Platform 11.1.0.3:

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

For upgrade paths supported for 11.1.0.0, see the *Upgrade Guide for Version 11.0.x to 11.1*.

You can update 11.1.0.3 patch using one of the following options:

- If the NetWitness Server has internet connectivity to Live Services, the NetWitness Suite User Interface can be used to apply the patch.
- If the NetWitness Server does not have internet connectivity to Live Services, the Command Line Interface (CLI) can be used to apply the patch.

## Update Tasks

You can choose one of the following update methods based on your internet connectivity.

### Online Method (Connectivity to Live Services): Update Using NetWitness User Interface

You can use this method if the NetWitness Server is connected to Live Services and can obtain the package.

**Note:** If the NetWitness Server does not have access to Live Services, use [Offline Method \(No connectivity to Live Services\): Update using the Command Line Interface](#) .

### Prerequisites

Make sure that:

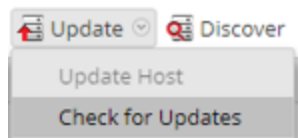
1. The “Automatically download information about new updates every day” option is checked and is applied in **ADMIN > System > Updates** .
2. Go to **ADMIN > Hosts > Update > Check for Updates** to check for updates. The Host page displays the **Update Available** status.
3. 11.1.0.3 is available under “Update Version” column.


**Note:** If you have custom certs, move any custom certs from `/etc/pki/nw/trust/import/` directory to `/root/cert`. Follow these steps to move the certs:

- 1.) `mkdir /root/cert.`
- 2.) `mv /etc/pki/nw/trust/import/* /root/cert.`

## Procedure

1. Go to **ADMIN > Hosts**.
2. Select the NetWitness Server (nw-server) host.
3. Check for the latest updates.



4. **Update Available** is displayed in the **Status** column if you have a version update in your Local Update Repository for the selected host.
5. Select **11.1.0.3** from the **Update Version** column.  
If you:
  - Want to view a dialog with the major features in the update and information on the updates, click the information icon (  ) to the right of the update version number.
  - Cannot find the version you want, select **Update > Check for Updates** to check the repository for any available updates. If an update is available, the message "New updates are available" is displayed and the **Status** column updates automatically to show **Update Available**. By default, only supported updates for the selected host are displayed.
6. Click **Update > Update Host** from the toolbar.
7. Click **Begin Update**.
8. Click the **Reboot Host**.
9. Repeat steps 6 to 8 for other hosts.

**Note:** You can select multiple hosts to update at the same time only after updating and rebooting the NetWitness Admin server. All ESA, Endpoint Insights, and Malware hosts should be updated to the same version as that of NW Admin Server or NetWitness Admin Server.

**Note:** Not all components have been changed for 11.1.0.3, so after you perform the update steps, it is normal to see some components with different version numbers. For a list of the components that were updated for this release, see [Build Numbers](#).

## Offline Method (No connectivity to Live Services): Update using the Command Line Interface

You can use this method if the NetWitness Server is not connected to Live Services.

**Note:** The update instructions for 11.x must be followed carefully to avoid corrupting the upgrade process. If you are familiar with the upgrade procedure for 10.x, be especially careful to follow these instructions and do not attempt to update as you would have updated 10.x.

### Prerequisites

Make sure that:

- You have downloaded the following file, which contain all the NetWitness Suite 11.1.0.3 update files, from RSA Link (<https://community.rsa.com/>) > NetWitness Suite > RSA NetWitness Logs and Packets Downloads to a local directory:

```
netwitness-11.1.0.3.zip
```

Upgrading from:	Download and Stage File:
11.1.0.0	netwitness-11.1.0.1.zip, netwitness-11.1.0.2.zip, and netwitness-11.1.0.3.zip
11.1.0.1	netwitness-11.1.0.2.zip, and netwitness-11.1.0.3.zip
11.1.0.2	netwitness-11.1.0.3.zip

### Procedure

You need to perform the update steps for NW Admin servers and for component servers.

**Note:** If you are updating from version 11.1.0.0, perform step 1 to create a `/tmp/upgrade/11.1.0.1` directory for the 11.1.0.1 files. Step 2 to create a `/tmp/upgrade/11.1.0.2` directory for the 11.1.0.2 files, in addition to creating a `/tmp/upgrade/11.1.0.3` directory for the 11.1.0.3 files.

**Note:** If you update from 11.1.0.1 version to 11.1.0.3, you must stage 11.1.0.2 files along with 11.1.0.3 files.

**Note:** If you copy paste the commands from PDF to Linux SSH terminal, the characters don't work. It is recommended to type the commands.

- Stage 11.1.0.3 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.1.0.3` and extract the zip package.

```
unzip netwitness-11.1.0.3.zip -d /tmp/upgrade/11.1.0.3
```



**Note:** If you copied the .zip file to the created staging directory to unzip, make sure that you delete the initial .zip file that you copied to the staging location after you extract it.

2. (Conditional) Stage 11.1.0.2 by creating a directory on the NetWitness Server at /tmp/upgrade/11.1.0.2 and extract the zip package. `unzip netwitness-11.1.0.2.zip -d /tmp/upgrade/11.1.0.2`
3. (Conditional) Stage 11.1.0.1 by creating a directory on the NetWitness Server at /tmp/upgrade/11.1.0.1 and extract the zip package. `unzip netwitness-11.1.0.1.zip -d /tmp/upgrade/11.1.0.1`
4. Initialize the update, using the following command:  
`upgrade-cli-client --init --version 11.1.0.3 --stage-dir /tmp/upgrade`
5. Update Netwitness Server, using the following command:  
`upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.1.0.3`
6. When the component host update is successful, reboot the host from NetWitness UI.
7. Repeat steps 3 and 4 for each component host, changing the IP address to the component host which is being updated.

**Note:** You can check versions of all the hosts, using the command `upgrade-cli-client --list` on NetWitness Server. If you want to view the help content of `upgrade-cli-client`, use the command `upgrade-cli-client --help`.

**Note:** If the following error displays during the update process:

```
2017-11-02 20:13:26.580 ERROR 7994 - [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
the patch will install correctly. No action is required. If you encounter additional errors when updating a
host to a new version, contact Customer Support (Contacting Customer Care).
```

**Note:** To Enable Respond Server, you need update ESA Primary and restart the Respond server.

## External Repo Instructions for CLI Update

**Note:** External repo which is to be setup should have 11.1.0.3 repo set under the same directory as 11.1.0.0.

1. Stage 11.1.0.3 by creating a directory on the NetWitness Server at /tmp/upgrade/11.1.0.3 and extract the zip package.  
`unzip netwitness-11.1.0.3.zip -d /tmp/upgrade/11.1.0.3`

**Note:** If you copied the .zip file to the created staging directory to unzip, make sure that you delete the initial .zip file that you copied to the staging location after you extract it.

2. Initialize the update, using the following command:

```
upgrade-cli-client --init --version 11.1.0.3 --stage-dir /tmp/upgrade
```

3. Update NetWitness Server, using the following command:

```
upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.1.0.3
```

4. When the component host update is successful, reboot the host from NetWitness UI.
5. Repeat steps 3 and 4 for each component host, changing the IP address to the component host which is being updated.

**Note:** You can check versions of all the hosts, using the command `upgrade-cli-client --list` on NetWitness Server. If you want to view the help content of `upgrade-cli-client`, use the command `upgrade-cli-client --help`.

**Note:** If the following error displays during the update process:

```
2017-11-02 20:13:26.580 ERROR 7994 - [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```

the patch will install correctly. No action is required. If you encounter additional errors when updating a host to a new version, contact Customer Support ([Contacting Customer Care](#)).

**Note:** To Enable Respond Server, you need update ESA Primary and restart the Respond server.

## Post-Update Tasks

### Task 1 (Optional) - Move the custom certs

Move the custom certs from external directory to `/etc/pki/nw/trust/import` directory.

### Task 2 (Conditional) - Reconfigure PAM Radius Authentication

If you configured PAM Radius authentication in 11.1.x.x using the `pam_radius` package, you must reconfigure it in 11.1.0.3 using the `pam_radius_auth` package.

You need to execute the below commands on NW Server on which the Admin server resides.

**Note:** If you have configured `pam_radius` in 11.x.x.x, perform the below steps to uninstall the existing version, or you can proceed with Step 2.

Step 1: Verify the existing page and uninstall the existing `pam_radius`

```
rpm -qi |grep pam_radius
yum erase pam_radius
```

Step 2: To install the `pam_radius_auth` package, excute the following command

```
yum install pam_radius_auth
```

Step 3: Edit the RADIUS configuration file, `/etc/raddb/server` as follows and add the configurations for radius server:

```
# server[:port] shared_secret timeout (s)
server secret 3
```

For example - 111.222.33.44 secret 1

Step 4: Edit the NetWitness Server PAM configuration file `/etc/pam.d/securityanalytics` to add the following line. If the file does not exist, create it and add the following line:

```
auth sufficient pam_radius_auth.so
```

Step 5: Provide the write permission to `/etc/raddb/server` files using below command

```
chown netwitness:netwitness /etc/raddb/server
```

Step 6: To copy the `pam_radius_auth` library, execute the following command

```
cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
```

Step 7: Restart the jetty server after making the changes to `pam_radius_auth` configurations, excute the following command.

```
systemctl restart jetty
```

### **Task 3 - Restart the Respond Server**

Restart the Respond server:

```
systemctl restart rsa-nw-respond-server
```

## Fixed Issues

---

This section lists issues fixed since the last major release.

### Security Fixes

Tracking Number	Description
SACE-9687	Open redirect vulnerability on Login.

### Server Fixes

Tracking Number	Description
SACE-9430	After NetWitness 11.x.x.x update, unable to edit the custom feed URL
SACE-9946	An error message "IncorrectResultSizeDataAccessException" is displayed due to authentication failure in LDAP.

### Investigate Fixes

Tracking Number	Description
SACE-9874	Unable to view recent queries on the Investigate view.
SACE-9691	On the Event Analysis view, the Services drop-down list does not have Scroll bar due to which the complete list is not displayed.
SACE-9144	When you investigate a specific query, the metadata is displayed in the Navigate view but not in the Events view.

### Core Fixes

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

Tracking Number	Description
SACE-9481	An error message is consuming Logs from Concentrator.

SACE-10027

After you upgrade to 11.1.0.2, the VLAN tags are missing from metadata.

## 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.

**Note:** The known issues from the previous releases of 11.1.0.0 may be fixed in the service packs. Refer to the respective service pack or patch release notes that are available on RSA Link: <https://community.rsa.com/>.

### Server

#### Custom STIX Recurring feed URL field is editable

**Tracking Number:** ASOC-62361

**Problem:** Live Feed configuration allows you to edit the STIX Recurring feed URL even after the configuration is successful. Upon editing custom feed, the custom feed creation does not change and uses the previous URL.

**Workaround:** None.

#### Login operation is generating logout audit log

**Tracking Number:** ASOC-62750

**Problem:** When you generate audit logs for login operation, the audit logs displays logout operation.

**Workaround:** None.


### Respond

#### Aggregation Stops after Reconnection to Mongo

**Tracking Number:** ASOC-50911

**Problem:** After configuring the Mongo database and rebooting the ESA server, incidents are not being created.

**Workaround:** After configuring the Mongo database and rebooting the ESA server, restart the Respond Server service. Perform any one of the following options:

- From the command line: `systemctl restart rsa-nw-respond-server`
- From NetWitness Suite: Go to **ADMIN > Services**, select the Respond Server service, and then select  > Restart.

## Product Documentation

The following documentation is provided with this release.

Document	Location
RSA NetWitness Platform 11.1.0.0 Online Documentation	<a href="https://community.rsa.com/community/products/netwitness/111">https://community.rsa.com/community/products/netwitness/111</a>
RSA NetWitness Platform 11.1.0.0 Upgrade Instructions	<a href="https://community.rsa.com/community/products/netwitness/111">https://community.rsa.com/community/products/netwitness/111</a>
RSA NetWitness Platform 11.1.0.0 Upgrade Checklist	<a href="https://community.rsa.com/community/products/netwitness/111">https://community.rsa.com/community/products/netwitness/111</a>
RSA NetWitness Platform Hardware Setup Guides	<a href="https://community.rsa.com/community/products/netwitness/hardware-setup-guides">https://community.rsa.com/community/products/netwitness/hardware-setup-guides</a>
RSA Content for RSA NetWitness Platform	<a href="https://community.rsa.com/community/products/netwitness/rsa-content">https://community.rsa.com/community/products/netwitness/rsa-content</a>

## Contacting Customer Care

---

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

RSA Link	<a href="https://community.rsa.com/">https://community.rsa.com/</a>
Phone	1-800-995-5095, option 3
International Contacts	<a href="http://www.emc.com/support/rsa/contact/phone-numbers.htm">http://www.emc.com/support/rsa/contact/phone-numbers.htm</a>
Community	<a href="https://community.rsa.com/community/rsa-customer-support">https://community.rsa.com/community/rsa-customer-support</a>
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.

## Preparing to Contact 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 Suite product or application you are using.
- The type of hardware you are using.



## Revision History

Revision	Date	Description
0.1	14-Aug	First Draft