



Release Notes

for RSA NetWitness Platform 11.3.0.1



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

Release Notes	5
Fixed Issues	5
Upgrade Fixes	5
Health and Wellness Fixes	5
Respond Fixes	5
UEBA Fixes	6
Endpoint Fixes	6
Archiver Fixes	6
Build Numbers	7
Update Instructions	7
Update Tasks	8
Task 1: Disable Decoder Services	8
Task 2: Update the Patch	8
Online Method (Connectivity to Live Services): Update Using NetWitness User Interface	8
Prerequisites	8
Procedure	9
Offline Method (No connectivity to Live Services): Update using the Command Line Interface	10
Prerequisites	10
Procedure	10
External Repo Instructions for CLI Update	11
Post-Update Tasks	12
Task 1 - Update HIVE version	12
Task 2 (Optional) - Move the custom certs	12
Task 3 (Conditional) - Reconfigure PAM Radius Authentication	12
Task 4 - Restart the Respond Server	13
Product Documentation	15
Known Issues	15
Feedback on Product Documentation	15
Contacting Customer Care	15
Preparing to Contact Customer Care	16

Revision History 16

Release Notes

This document lists the fixes in NetWitness Platform 11.3.0.1. Read this document before deploying or updating NetWitness Platform 11.3.0.1

Fixed Issues

This document lists issues fixed in NetWitness Platform 11.3.0.1.

Upgrade Fixes

Tracking Number	Description
SACE-11250	In cases where systems have gone through multiple kernel updates, the <code>/boot</code> directory contained multiple kernel images, which consumed the <code>/boot</code> partition.

Health and Wellness Fixes

Tracking Number	Description
SACE-10840	<p>The following NetWitness Database (NW DB) retention statistics are now available in 11.3.0.1</p> <ul style="list-style-type: none">• Overall Meta Oldest File Time Retention• Overall Session Oldest File Time Retention• Overall Packet Oldest File Time Retention

Respond Fixes

Tracking Number	Description
ASOC-75674	When you update to 11.3, Respond's primary host property (<code>/rsa/primary/host</code>) was set to <code>false</code> by default, which had an adverse effect on some of the critical functionality. This is now set as <code>true</code> .

UEBA Fixes

Tracking Number	Description
ASOC-75673	The cache size for MongoDB is set to 20 GB for better performance.
ASOC-73271	The OOTB UEBA Incident Rule was missing UEBA values in the <code>Source</code> and <code>GroupBy</code> fields.

Endpoint Fixes

Tracking Number	Description
ASOC-74735	Owner information is now available on the Hosts > Details > Process tab.
ASOC-73742	A complete list of Loaded Libraries was not displayed when investigating the process.
ASOC-74199	On Windows, the agent driver stopped when the agent mode was changed multiple times from <code>Advanced</code> to <code>Insights</code> .
ASOC-74025	The Endpoint agent was not able to communicate to the server using UDP when it went back to HTTP mode.
ASOC-72823	The default scan schedule is now set to 1 week for improved performance of the Endpoint Server.

Archiver Fixes

Tracking Number	Description
ASOC-74691	When you included a meta value in the Archiver configuration, the <code>metakey word</code> was also added.

Build Numbers

The following table lists the build numbers for various components of NetWitness Platform 11.3.0.1.

Component	Version Number
NetWitness Platform Decoder	11.3.0.1-9760.5
NetWitness Platform Concentrator	11.3.0.1-9760.5
NetWitness Platform Broker	11.3.0.1-9760.5
NetWitness Platform Log Decoder	11.3.0.1-9760.5
NetWitness Platform Archiver (Workbench)	11.3.0.1-9760.5
NetWitness Platform Appliance	11.3.0.1-9760.5
NetWitness Platform Console	11.3.0.1-9760.5
NetWitness Platform Endpoint Agents	11.3.0.1-1904041524.5
NetWitness Platform Endpoint Server	11.3.0.1-190410132138.5
NetWitness Platform Legacy Web Server	11.3.0.1-190429134525.5
NetWitness Platform Log Player	11.3.0.1-9760.5
NetWitness Platform Respond Server	11.3.0.1-190429095829.5
NetWitness Platform SDK	11.3.0.1-9760.5

Update Instructions

You need to read the information and follow these procedures for updating NetWitness Platform version 11.3.0.1.

The following update paths are supported for NetWitness Platform 11.3.0.1:

- NetWitness Platform 11.1.x.x to 11.3.0.1
- NetWitness Platform 11.2.x.x to 11.3.0.1
- NetWitness Platform 11.3.0.0 to 11.3.0.1

To update NetWitness Platform from 11.1.x.x or 11.2.x.x, you must download files for the 11.3.0.0 base release and the 11.3.0.1 patch release. To update from 11.3.0.0 to 11.3.0.1, you only need to download files for the 11.3.0.1 patch release.

For update paths supported for 11.3.0.0, see the *Update Guide for Version 11.x.x.x to 11.3*.

You can update 11.3.0.1 patch using one of the following options:

- If the NetWitness Server has internet connectivity to Live Services, the NetWitness Platform 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

Task 1: Disable Decoder Services

Before updating to 11.3.0.1, you must disable Capture AutoStart on Network Decoder and Network Hybrid Services.

To disable the Capture Autostart field:

1. Go to **ADMIN > Services**.

The Administration Services view is displayed.

2. Select a Network Decoder or Network Hybrid service and select  > **View > Config**.

The services config view for the selected Network Decoder or Network Hybrid is displayed.

3. In the **Decoder Configuration** panel, deselect the **Capture Autostart** field and click **Apply**.

Task 2: Update the Patch

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:

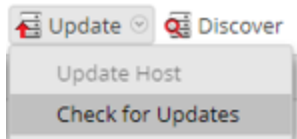
1. The “Automatically download information about new updates every day” option is checked and is applied in **ADMIN > System > Updates** .
2. Go to **ADMIN > Hosts > Update > Check for Updates** to check for updates. The Host page displays the **Update Available** status.
3. 11.3.0.1 is available under “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 **11.3.0.1** 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, and Malware Analysis 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 11.3.0.1, 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.

Prerequisites

Make sure that you have downloaded the following files, which contain all the NetWitness Platform 11.3.0.1 update files, from RSA Link (<https://community.rsa.com/>) > NetWitness Platform > RSA NetWitness Logs and Network > Downloads > RSA Downloads to a local directory:

- If you are updating from an 11.1.x.x or an 11.2.x.x release, download `netwitness-11.3.0.0.zip` and `netwitness-11.3.0.1.zip`.
- If you are updating from 11.3.0.0, download `netwitness-11.3.0.1.zip`.

Procedure

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

Note: If you copy paste the commands from PDF to Linux SSH terminal, the characters do not work. It is recommended to type the commands.

1. **If you are updating from 11.1.x.x or 11.2.x.x**, you must stage 11.3.0.0 and 11.3.0.1. Log into the `/root` directory of the Admin NetWitness Server and create the following directories:
`/tmp/upgrade/11.3.0.0`
`/tmp/upgrade/11.3.0.1`
 and then copy the package zip files to the `/root` directory of the Admin server and extract the package files from `/root` to the appropriate directories:
`unzip netwitness-11.3.0.0.zip -d /tmp/upgrade/11.3.0.0`
`unzip netwitness-11.3.0.1.zip -d /tmp/upgrade/11.3.0.1`
2. **If you are updating from 11.3.0.0 to 11.3.0.1**, you only need to stage 11.3.0.1. Log into the `/root` directory of the Admin NetWitness Server and create the following directory:
`/tmp/upgrade/11.3.0.1`
 and then copy the package zip files to the `/root` directory of the Admin server and extract the package

files from /root to the /tmp/upgrade/11.3.0.1 directory:

```
unzip netwitness-11.3.0.1.zip -d /tmp/upgrade/11.3.0.1
```

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.

3. Initialize the update, using the following command:

```
upgrade-cli-client --init --version 11.3.0.1 --stage-dir /tmp/upgrade
```

4. Update Netwitness Server, using the following command:

```
upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version  
11.3.0.1
```

5. When the component host update is successful, reboot the host from NetWitness UI.
6. Repeat steps 4 and 5 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 the 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).
```

External Repo Instructions for CLI Update

Note: The external repo should have separate directories for 11.3.0.0 and 11.3.0.1, as described in [Offline Method \(No connectivity to Live Services\): Update using the Command Line Interface](#).

1. Stage 11.3.0.1 by creating a directory on the NetWitness Server at /tmp/upgrade/11.3.0.1 and extract the zip package.

```
unzip netwitness-11.3.0.1.zip -d /tmp/upgrade/11.3.0.1
```

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 11.3.0.1 --stage-dir /tmp/upgrade
```

3. Update Netwitness Server, using the following command:

```
upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version
11.3.0.1
```

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).
```

Post-Update Tasks

Task 1 - Update HIVE version

After you update to 11.3.0.1, you need to update the HIVE version that is compatible with Warehouse. To install the latest HIVE version, run the following commands on the NetWitness admin server and restart the Reporting Engine service.

1. To install HIVE 0.12 version, run the following command:

```
rpm -ivh rsa-nw-hive-jdbc-0.12.0-1.x86_64.rpm
```
2. To Install HIVE 1.0 version, run the following command:

```
rpm -ivh rsa-nw-hive-jdbc-1.0.0-1.x86_64
```

Task 2 (Optional) - Move the custom certs

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

Task 3 (Conditional) - Reconfigure PAM Radius Authentication

If you configured PAM Radius authentication in 11.3x.x using the `pam_radius` package, you must reconfigure it in 11.3.0.1 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` package.

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

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

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

Step 6: To copy the `pam_radius_auth` library, run 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 and run the following command.

```
systemctl restart jetty
```

Task 4 - Restart the Respond Server

Restart the Respond server:

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

To enable the Capture Autostart field:

1. Go to **ADMIN > Services**.

The Administration Services view is displayed.

2. Select a Network Decoder or Network Hybrid service and select  > **View > Config**.

The services Config view for the selected Network Decoder or Network Hybrid is displayed.

3. In the **Decoder Configuration** panel, select the **Capture Autostart** field and click **Apply**.

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA NetWitness Platform 11.3.0.0 Online Documentation	https://community.rsa.com/community/products/netwitness/113

Known Issues

Issues that remain unresolved in this release are documented here:

<https://community.rsa.com/community/products/netwitness/documentation/known-issues>. Wherever a workaround is available, it is noted or referenced in detail.

Feedback on Product Documentation

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

Contacting Customer Care

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

RSA Link	https://community.rsa.com/
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/rsa-customer-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.

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

Revision History

Revision	Date	Description
0.1	13-May	Final Draft