



# RSA<sup>®</sup> NetWitness Platform

Version 11.6.0.1

## Release Notes



## Contact Information

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

## Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

## License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and 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 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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("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.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

July 2021

# Contents

---

<b>What's New</b> .....	<b>5</b>
GPG Key Changes .....	5
Upgrade Paths .....	5
Security Fixes .....	5
<b>Fixed Issues</b> .....	<b>6</b>
Context Hub Fixes .....	6
Log Collection Fixes .....	6
Investigate Fixes .....	6
Core Services (Broker, Concentrator, Decoder, Archiver) Fixes .....	7
Event Stream Analysis (ESA) Fixes .....	7
Reporting Engine Fixes .....	7
Respond Fixes .....	8
<b>Upgrade Instructions</b> .....	<b>9</b>
Running in Mixed Mode .....	9
<b>Upgrade Tasks</b> .....	<b>10</b>
Important Notes - Read This First .....	10
Synchronize Time on Component Hosts with NW Server Host .....	10
Mixed Mode Unsupported for ESA Hosts .....	10
Respond Server Service Not Enabled Until NW Server and Primary ESA Host Upgraded to 11.6.0.1 .....	10
Task 1: Upgrade External Repository .....	10
Task 2: Disable Decoder Services .....	11
Task 3: Upgrade the Patch .....	11
<b>Upgrade Options</b> .....	<b>13</b>
Option 1: Online Method (Connectivity to Live Services): Upgrade Using NetWitness Platform User Interface .....	13
Prerequisites .....	13
Procedure .....	14
Option 2: Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface .....	14
Download the 11.6.0.1 Patch .....	15
Procedure .....	15
External Repo Instructions for CLI Upgrade .....	17
Option 3: Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface .....	18
<b>Post-Upgrade Tasks</b> .....	<b>19</b>
Post Upgrade Tasks for Customers Upgrading from version 11.6.0.0 .....	19
Task 1 (Optional) - Move the custom certificates .....	19

---

Task 2- Enable Decoder Services .....	19
Post Upgrade Tasks for Customers Upgrading from version 11.4.1.4 or 11.5.3.2 .....	19
<b>Getting Help with NetWitness Platform .....</b>	<b>20</b>
Self-Help Resources .....	20
Contact RSA Support .....	20
<b>Product Documentation .....</b>	<b>21</b>
Feedback on Product Documentation .....	21
<b>Build Numbers .....</b>	<b>22</b>
<b>Appendix A. Offline Method (No connectivity to Live Services): .....</b>	<b>23</b>
Upgrade using the NetWitness Platform User Interface. ....	23
Download the 11.6.0.1 Patch .....	23
<b>Revision History .....</b>	<b>25</b>

# What's New

---

The RSA NetWitness Platform 11.6.0.1 release notes provides information about the changes in NetWitness Platform 11.6.

## GPG Key Changes

The GPG Signing for NetWitness has changed for releases beyond 11.6.0.0. In order to upgrade to 11.6.0.1 release, you must first upgrade to a version that is signed by the old GPG key but contains the new GPG key. For more information, see [GPG Key Change in NetWitness Platform Beyond 11.6.0.0](#).

## Upgrade Paths

The following upgrade paths are supported for NetWitness Platform 11.6.0.1:

- RSA NetWitness Platform 11.4.1.4 to 11.6.0.1
- RSA NetWitness Platform 11.5.3.2 to 11.6.0.1
- RSA NetWitness Platform 11.6.0.0 to 11.6.0.1

## Security Fixes

For more information on Security Fixes, see [Security Advisories](#).

## Fixed Issues

---

This section lists issues fixed after the last major release. For additional information on fixed issues, see the Fixed Version column in the [RSA NetWitness® Platform Known Issues list](#) on RSA Link.

### Context Hub Fixes

Tracking Number	Description
ASOC-111209	In the <b>Add Data Source</b> window, when you edit a value (such as password), the UI <b>With Column Headers</b> is grayed out. Consequently, the first value in the list loaded from the CSV file will be considered as the header row data and it was deleted.

### Log Collection Fixes

Tracking Number	Description
ASOC-110086	When you send logs to Log Decoder and Virtual Log Collector, the logs sent to Log Decoder are received immediately on the Investigation page. However, log collection is delayed when logs are sent to the Virtual Log Collector. Debug error message such as <code>An error occurred publishing to an AMQP channel, exchange: syslog, routing key: syslog: a SSL error occurred</code> appears while collecting events.

### Investigate Fixes

Tracking Number	Description
ASOC-111211	In the <b>Filter Events</b> page, meta key values are displayed even when the DefaultAction parameter is defined as closed in the Services Index file.

## Core Services (Broker, Concentrator, Decoder, Archiver)

### Fixes

Tracking Number	Description
ASOC-111196	Files captured in the <b>Events</b> window are exported with wrong/invalid extensions in their filenames. Files with the extension such as .xslm appear as <code>&lt;filename.xslm.docx&gt;</code> when you download them from the Decoder service.

### Event Stream Analysis (ESA) Fixes

Tracking Number	Description
ASOC-111212	While creating custom feeds, the meta keys are not displayed accurately. Information such as netname, ip.org are unavailable, as it does not retrieve information from all the services that are selected for the feed deployment.
ASOC-111208	After upgrading to Esper 8.4 version, ESA rule error such as <code>STOP_ALL_RULE_PROCESSING_AND_WAIT</code> appears. Alerts are not triggered and ESA performance is affected.
ASOC-111264	When you download Event Sources (which appear in the <b>Manage</b> tab), the last seen time in the CSV file is displayed in the epoch format and not in UTC or IST format.

### Reporting Engine Fixes

Tracking Number	Description
ASOC-111215	While creating new alerts in the <b>Reports</b> tab, if you select <b>Push to decoders</b> , the error message No decoders are configured for the selected data source to add the alert rule is displayed. Consequently, alerts are not triggered.
ASOC-111261	While creating a chart and report for a particular rule over the same period of time, the output (chart and report) does not match. This is due to an unexpected error that occurs when parsing data into the dashlets.

## Respond Fixes

Tracking Number	Description
ASOC-111219	Risk score for alerts fail as specific files cannot be identified. When you calculate the risk score, the system displays the following error message as the file identity is not a part of the alert information sent by ESA, Endpoint, Malware, or Report data sources to the Respond server:[ <code>alert-processing-pipeline</code> ] ERROR RiskScoring No File found to calculate score for Alert : Gets Current User As SYSTEM.
ASOC-111348	Explore page does not load after selecting <b>View &gt; Explore</b> under <b>Actions</b> in the <b>Services</b> window. As a result, data such as configuration, metrics are unavailable.



# Upgrade Instructions

---

You need to read the information and follow these procedures for upgrading NetWitness Platform version 11.6.0.1.

Upgrade Path	Downloads Required
From 11.4.1.4 to 11.6.0.1	<ul style="list-style-type: none"><li>• 11.6.0.0 base pack</li><li>• 11.6.0.1 patch release</li></ul>
From 11.5.3.2 to 11.6.0.1	<ul style="list-style-type: none"><li>• 11.6.0.0 base pack</li><li>• 11.6.0.1 patch release</li></ul>
From 11.6.0.0 to 11.6.0.1	<ul style="list-style-type: none"><li>• 11.6.0.1 patch release</li></ul>

You can upgrade 11.6.0.1 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) or the NetWitness Platform User Interface can be used to apply the patch.

**Note:** If you are using S4s device that utilizes SD cards, SSH to NW Server and run the following command before starting the upgrade process. `manage-stig-controls --disable-control-groups 7 --host-id <node uuid>`.

For upgrading from 11.4.1.4 or 11.5.3.2, see the *RSA NetWitness Platform 11.6 Upgrade Guide*.

## Running in Mixed Mode

Running in mixed mode occurs when some services are upgraded to the latest version and some services are on older versions. See "Running in Mixed Mode" in the *RSA NetWitness Platform Hosts and Services Getting Started Guide* for further information.

**Note:** If you are running Endpoint Log Hybrid in mixed mode, make sure Endpoint Broker is on the same version as one of the Endpoint Servers.

## Upgrade Tasks

---

### Important Notes - Read This First

#### Synchronize Time on Component Hosts with NW Server Host

Before upgrading your hosts, make sure that the time on each host is synchronized with the time on the NetWitness Server.

To synchronize the time, do one of the following:

- Configure the NTP Server. For more information, see "Configure NTP Servers" in the *System Configuration Guide*.
- Perform the following steps on each host:
  - a. SSH to a component host.
  - b. Run the following commands.

```
systemctl stop ntpd
ntpdate nw-node-zero
systemctl start ntpd
```

#### Mixed Mode Unsupported for ESA Hosts

Mixed mode is not supported for ESA hosts in NetWitness Platform version 11.5 and later. The NetWitness server, ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

#### Respond Server Service Not Enabled Until NW Server and Primary ESA Host Upgraded to 11.6.0.1

After upgrading the primary NW Server (including the Respond Server service), the Respond Server service is not automatically re-enabled until after the Primary ESA host is also upgraded to 11.6.0.1. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

#### Task 1: Upgrade External Repository

**Note:** Perform the below steps only if you are using an external repository for 11.6.0.1.

To upgrade the external repository which is an externally managed server, do the following:

1. Upgrade the external repository with the latest upgrade content for the RSA `netwitness-11.6.0.1.zip`.  
The following is the structure after upgrading the external repository:

```



|-11.5.3.2
|---OS
|-----reodata
|---RSA
|-----reodata
|-11.6.0.0
|---OS
|-----reodata
|---RSA
|-----reodata
|-11.6.0.1
|---OS
|-----reodata
|---RSA
|-----reodata
|-cloud-extras
|---RSA
|-----reodata

```

## Task 2: Disable Decoder Services

Before upgrading to 11.6.0.1, you must disable Capture AutoStart on Network Decoder and Network Hybrid Services.

### To disable Capture Autostart:

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** and click **Apply**.

## Task 3: Upgrade the Patch

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

- [Option 1: Online Method \(Connectivity to Live Services\): Upgrade Using NetWitness Platform User Interface](#)
- [Option 2: Offline Method \(No connectivity to Live Services\): Upgrade using the Command Line Interface](#)
- [Option 3: Offline Method \(No connectivity to Live Services\): Upgrade using the NetWitness Platform User Interface](#)

## Upgrade Options



### Option 1: Online Method (Connectivity to Live Services): Upgrade Using NetWitness Platform User Interface

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

**Note:** If the NetWitness Server does not have access to Live Services, use [Option 2: Offline Method \(No connectivity to Live Services\): Upgrade using the Command Line Interface](#) . or use [Option 3: Offline Method \(No connectivity to Live Services\): Upgrade using the NetWitness Platform User Interface](#)

### Prerequisites


Make sure that:

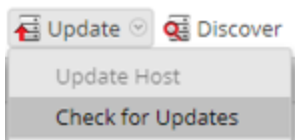
1. The **Automatically download information about new upgrades every day** option is selected and is applied in  (Admin) > System > Updates.
2. Go to  (Admin) > Hosts > Update > Check for Updates to check for upgrades. The Host page displays the **Update Available** status.
3. 11.6.0.1 is available under **Update Version** column.


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

- 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 upgrade in your Local Update Repository for the selected host.
5. Select **11.6.0.1** from the **Update Version** column. If you:
  - Want to view a dialog with the major features in the upgrade and information on the updates, click the information icon (  ) to the right of the upgrade 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 upgrades automatically to show **Update Available**. By default, only supported upgrades for the selected host are displayed.
6. Click **Update > Update Host** from the toolbar.
7. Click **Begin Update**.
8. Click the **Reboot Host** when prompted.
9. Repeat steps 6 to 8 for other hosts.

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

**Note:** Not all components have been changed for 11.6.0.1, so after you perform the upgrade steps, it is normal to see some components with different version numbers. For a list of the components that were upgraded for this release, see [Build Numbers](#).

## Option 2: Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface

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

**Note:** Alternatively, you can upgrade using the [Option 3: Offline Method \(No connectivity to Live Services\): Upgrade using the NetWitness Platform User Interface](#)

## Download the 11.6.0.1 Patch

Download the RSA NetWitness Platform 11.6.0.1 Upgrade Pack file, which contain all the NetWitness Platform 11.6.0.1 upgrade files, from the RSA Link <https://community.rsa.com/t5/rsa-netwitness-platform/tkb-p/netwitness-downloads> to a local directory.

netwitness-11.6.0.1.zip

Upgrading from	Download and Stage file
11.4.1.4	netwitness-11.6.0.0.zip and netwitness-11.6.0.1.zip
11.5.3.2	netwitness-11.6.0.0.zip and netwitness-11.6.0.1.zip
11.6.0.0	netwitness-11.6.0.1.zip

**Note:** If you are using external repository, you can upgrade the external repository with the latest upgrade content. For more information see, [Task 1: Upgrade External Repository](#).

## Procedure

You need to perform the upgrade steps for NetWitness Server host and for component hosts.

**Note:** Ensure that you have enough space in the NetWitness Server root and tmp directory before you unzip the package files.

**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.

**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.

- If you are upgrading from 11.4.1.4 to 11.6.0.1**, you only need to stage 11.6.0.0 and 11.6.0.1. Log into the /root to the directory of the NetWitness Server and create the following directory:

```
/tmp/upgrade/11.6.0.0
/tmp/upgrade/11.6.0.1
```

and then copy the package zip files to the /root directory of the NetWitness Server and extract the package files from /root to the /tmp/upgrade/11.6.0.1 directory:

```
unzip netwitness-11.6.0.0.zip -d /tmp/upgrade/11.6.0.0
unzip netwitness-11.6.0.1.zip -d /tmp/upgrade/11.6.0.1
```
- If you are upgrading from 11.5.3.2 to 11.6.0.1**, you only need to stage 11.6.0.0 and 11.6.0.1. Log into the /root to the directory of the NetWitness Server and create the following directory:

```
/tmp/upgrade/11.6.0.0
/tmp/upgrade/11.6.0.1
```

and then copy the package zip files to the /root directory of the NetWitness Server and extract the package files from /root to the /tmp/upgrade/11.6.0.1 directory:

```
unzip netwitness-11.6.0.0.zip -d /tmp/upgrade/11.6.0.0
unzip netwitness-11.6.0.1.zip -d /tmp/upgrade/11.6.0.1
```

- **If you are upgrading from 11.6.0.0 to 11.6.0.1**, You only need to stage 11.6.0.1. There are two options to stage 11.6.0.1.
  - **Option 1 (Manual)** : Log into the /root to the directory of the NetWitness Server and create the following directory:  
`/tmp/upgrade/11.6.0.1`  
and then copy the package zip files to the /root directory of the NetWitness Server and extract the package files from /root to the /tmp/upgrade/11.6.0.1 directory:  
`unzip netwitness-11.6.0.1.zip -d /tmp/upgrade/11.6.0.1`
  - **Option 2 (Automated)** : Log into the /root to the directory of the NetWitness Server and create the following directory:

```
/tmp/upgrade and /root/NW
```

and then copy the NetWitness 11.6.0.1 package zip files to the /root/NW directory of the NetWitness Server.

After this, run the below command to extract, validate, and initialize the 11.6.0.1 zip files:

```
[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --download-path <download file path> --version 11.6.0.1
```

Here, <download file path> is the location where you need to copy the **netwitness-11.6.0.1.zip** if it is downloaded to the local directory earlier.

For Example: `[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --download-path /root/NW --version 11.6.0.1`

Once the message **(INFO) Download and extraction of all the necessary NetWitness zips are completed** is displayed in the console of the admin server, only then the initialization process will begin.

**Note:** If you do not receive the message **(INFO) Download and extraction of all the necessary NetWitness zips are completed**, run the command `[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --download-path <download file path> --version 11.6.0.1` again to stage 11.6.0.1.

**Note:** After staging 11.6.0.1 (using the Option 2), if the initialization fails, run the command `upgrade-cli-client --init --version 11.6.0.1 --stage-dir /tmp/upgrade`. If the initialization succeeds, ignore the [first step](#) under **Upgrading the NetWitness Server and component hosts** and proceed with the further steps in it.



## Upgrading the NetWitness Server and component hosts

1. Initialize the upgrade, using the following command:  

```
upgrade-cli-client --init --version 11.6.0.1 --stage-dir /tmp/upgrade
```

**IMPORTANT:** Once *init* is performed, do not reboot the NW Admin server or restart jetty.

2. Upgrade Netwitness Server, using the following command:  

```
upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.6.0.1
```

3. When the component host upgrade is successful, reboot the host from NetWitness UI.

**IMPORTANT:** This is a mandatory step. Ensure that you reboot the host from the NetWitness UI.

4. Repeat steps 2 and 3 for each component host, changing the IP address to the component host which is being upgraded.

**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 upgrade 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 upgrading a host to a new version, contact [Upgrade Instructions](#).

## External Repo Instructions for CLI Upgrade

**Note:** The external repo should have separate directories for 11.6.0.0 and 11.6.0.1, as described in [Option 2: Offline Method \(No connectivity to Live Services\): Upgrade using the Command Line Interface](#)

**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.

1. Stage 11.6.0.1 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.6.0.1` and extract the zip package.  
`unzip netwitness-11.6.0.1.zip -d /tmp/upgrade/11.6.0.1`
2. Initialize the upgrade, using the following command:  
`upgrade-cli-client --init --version 11.6.0.1--stage-dir /tmp/upgrade`
3. Upgrade Netwitness Server, using the following command:  
`upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.6.0.1`
4. When the component host upgrade 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 upgraded.

**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 upgrade 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 upgrading a host to a new version, contact [Upgrade Instructions](#).

### Option 3: Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface

Follow the instructions in [Appendix A. Offline Method \(No connectivity to Live Services\): Upgrade using the NetWitness Platform User Interface](#).

---

## Post-Upgrade Tasks

---

This topic is divided into two sections, based on the version that you are upgrading from:

[Post Upgrade Tasks for Customers Upgrading from version 11.6.0.0](#)

[Post Upgrade Tasks for Customers Upgrading from version 11.4.1.4 or 11.5.3.2](#)

### Post Upgrade Tasks for Customers Upgrading from version 11.6.0.0



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

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

#### Task 2- Enable Decoder Services

After you upgrade to 11.6.0.1, you must enable Capture AutoStart on Network Decoder and Network Hybrid Services.

**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**.

### Post Upgrade Tasks for Customers Upgrading from version 11.4.1.4 or 11.5.3.2

Perform all the post upgrade tasks mentioned in *Upgrade Guide for RSA NetWitness Platform 11.6.0.0*.

# Getting Help with NetWitness Platform

---

## Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness Platform:

- See the documentation for all aspects of NetWitness Platform here:  
<https://community.rsa.com/community/products/netwitness/documentation>
- Use the **Search** and **Ask it** fields in RSA Link to find specific information here:  
<https://community.rsa.com/welcome>
- See the RSA NetWitness Platform Knowledge Base:  
<https://community.rsa.com/community/products/netwitness/knowledge-base>
- See Troubleshooting the RSA NetWitness Platform:  
<https://community.rsa.com/community/products/netwitness/documentation/troubleshooting>
- See also [RSA NetWitness® Platform Blog Posts](#).
- If you need further assistance, contact RSA Support.

## Contact RSA Support

If you contact RSA Support, you should be at your computer. Be prepared to provide 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	<a href="https://community.rsa.com">https://community.rsa.com</a> In the main menu, click <b>My Cases</b> .
International Contacts (How to Contact RSA Support)	<a href="https://community.rsa.com/docs/DOC-1294">https://community.rsa.com/docs/DOC-1294</a>
Community	<a href="https://community.rsa.com/community/support">https://community.rsa.com/community/support</a>

# Product Documentation

---

The following documentation is provided with this release.

Documentation	Location URL
RSA NetWitness Platform 11.x Master Table of Contents	<a href="https://community.rsa.com/t5/rsa-netwitness-platform/ct-p/netwitness-documentation">https://community.rsa.com/t5/rsa-netwitness-platform/ct-p/netwitness-documentation</a>
RSA NetWitness Platform 11.6 Product Documentation	<a href="https://community.rsa.com/">https://community.rsa.com/</a>
RSA NetWitness Platform 11.6 Upgrade Guide	<a href="https://community.rsa.com/t5/rsa-netwitness-platform-online/upgrade-instructions-for-rsa-netwitness-platform-11-x-to-11-6/ta-p/606727">https://community.rsa.com/t5/rsa-netwitness-platform-online/upgrade-instructions-for-rsa-netwitness-platform-11-x-to-11-6/ta-p/606727</a>

## Feedback on Product Documentation

You can send an email to [nwdocsfeedback@rsa.com](mailto:nwdocsfeedback@rsa.com) to provide feedback on RSA NetWitness Platform documentation.

## Build Numbers

The following table lists the build numbers for various components of NetWitness Platform 11.6.0.1.

Component	Version Number
NetWitness Platform Appliance	11.6.0.1-12007.5
NetWitness Platform Archiver	11.6.0.1-12007.5
NetWitness Platform Bootstrap	11.6.0.1-2106031505.5
NetWitness Platform Broker	11.6.0.1-12007.5
NetWitness Platform Concentrator	11.6.0.1-12007.5
NetWitness Platform Config Management	11.6.0.1-2106031505.5
NetWitness Platform Console	11.6.0.1-12007.5
NetWitness Platform Decoder	11.6.0.1-12007.5
NetWitness Platform Deployment Upgrade	11.6.0.1-2106031506.5
NetWitness Platform Legacy Web Server	11.6.0.1-210625025340.5
NetWitness Platform Log Collector	11.6.0.1-14970.5
NetWitness Platform Log Decoder	11.6.0.1-12007.5
NetWitness Platform Log Player	11.6.0.1-12007.5
NetWitness Platform RE Server	11.6.0.1-5899.5
NetWitness Platform UI	11.6.0.1-210628060532.5
NetWitness Platform WorkBench	11.6.0.1-12007.5
NetWitness Platform Context Hub Server	11.6.0.1-210624161517.5
NetWitness Platform Correlation Server	11.6.0.1-210630045652.5
NetWitness Platform Investigate Server	11.6.0.1-210625040944.5
NetWitness Platform Malware Analytics Server	11.6.0.1-210625072240.5
NetWitness Platform Respond Server	11.6.0.1-210625061411.5
NetWitness Platform Component Descriptor	11.6.0.1-2107010307.5
NetWitness Platform Decoder Content	11.6.0.1-12007.5

# Appendix A. Offline Method (No connectivity to Live Services):

## Upgrade using the NetWitness Platform User Interface.

The following rules apply when you apply version upgrades:

- You must upgrade the NW Server host first.
- You can only apply a version that is compatible with the existing host version.

### Download the 11.6.0.1 Patch

Download the RSA NetWitness Platform 11.6.0.1 Upgrade Pack file, which contain all the RSA NetWitness Platform 11.6.0.1 upgrade files, from the RSA Link <https://community.rsa.com/t5/rsa-netwitness-platform/tkb-p/netwitness-downloads> to a local directory.

netwitness-11.6.0.1.zip

Upgrading from	Download and Stage file
11.4.1.4	netwitness-11.6.0.0.zip and netwitness-11.6.0.1.zip
11.5.3.2	netwitness-11.6.0.0.zip and netwitness-11.6.0.1.zip
11.6.0.0	netwitness-11.6.0.1.zip

**Note:** If you get the **Download Error**, see the [Troubleshooting](#) information for resolution.

### Task 1. Populate Staging Folder (/var/lib/netwitness/common/upgrade-stage/) with Version Updates

- If you are upgrading from 11.4.1.4 or later to 11.6.0.1, download the netwitness-11.6.0.0.zip and netwitness-11.6.0.1.zip, upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.5.3.2 to 11.6.0.1, download the netwitness-11.6.0.0.zip and netwitness-11.6.0.1.zip, upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.6.0.0 to 11.6.0.1, download the netwitness-11.6.0.1.zip, upgrade package from RSA Link to a local directory.

1. SSH to the NW Server host.
2. If you are upgrading from 11.4.1.4 or later to 11.6.0.1, copy netwitness-11.6.0.0.zip and netwitness-11.6.0.1.zip from the local directory to the /var/lib/netwitness/common/update-stage/ staging folder.  
sudo cp /tmp/netwitness-11.6.0.0.zip /var/lib/netwitness/common/update-stage/

```
sudo cp /tmp/netwitness-11.6.0.1.zip /var/lib/netwitness/common/update-stage/
```

3. If you are upgrading from 11.5.3.2 to 11.6.0.1, copy `netwitness-11.6.0.0.zip` and `netwitness-11.6.0.1.zip` from the local directory to the `/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:  

```
sudo cp /tmp/netwitness-11.6.0.0.zip /var/lib/netwitness/common/update-stage/
```

```
sudo cp /tmp/netwitness-11.6.0.1.zip /var/lib/netwitness/common/update-stage/
```


NetWitness Platform unzips the file automatically.
4. If you are upgrading from 11.6.0.0 to 11.6.0.1, copy `netwitness-11.6.0.1.zip` from the local directory to the `/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:  

```
sudo cp /tmp/netwitness-11.6.0.1.zip /var/lib/netwitness/common/update-stage/
```

NetWitness Platform unzips the file automatically.

### Task 2. Apply Updates from the Staging Area to Each Host

**Caution:** You must upgrade the NW Server host before upgrading any Non-NW Server host.

1. Log in to NetWitness Platform.
2. Go to  (Admin) > Hosts.  
Check for updates and wait for the update packages to be copied, validated, and ready to be initialized.
3. "Ready to initialize packages" is displayed if:
  - NetWitness Platform can access the update package.
  - The package is complete and has no errors.Refer to [Troubleshooting Version Installations and upgrades](#) for instructions on how to troubleshoot errors (for example, "Error deploying version <version-number>" and "Missing the following update package(s)," are displayed in the **Initiate Update Package for RSA NetWitness Platform** dialog.)
4. Click **Initialize Update**.  
  
It takes some time to initialize the packages because the files are large and need to be unzipped. After the initialization is successful, the **Status** column displays **Update Available** and you complete the rest of the steps in this procedure to finish the update of the host.
5. Click **Update** > **Update Hosts** from the toolbar.
6. Click **Begin Update** from the **Update Available** dialog.  
After the host is upgraded, it prompts you to reboot the host.
7. Click **Reboot** from the toolbar.



# Revision History

---

Date	Description
July 2021	Release to Operations