# RSA® NetWitness Platform

Version 11.5.3.2

# 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 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.



June 2021

# Contents


**Introduction** ..... **5**
Fixed Issues ..... 5
Security Fixes ..... 5
**What's New** ..... **6**
Enhancements ..... 6
Licensing and Packaging ..... 6
**Fixed Issues** ..... **7**
Security Fixes ..... 7
Administration Fixes ..... 7
Malware Fixes ..... 7
Respond Server Fixes ..... 7
Reporting Engine Fixes ..... 8
Context Hub Fixes ..... 8
SCL Fixes ..... 8
ESA Fixes ..... 8
Log Collector Fixes ..... 9
**End of Life Functionality** ..... **10**
End of Life Functionality and Features in 11.5.3.2 ..... 10
**Upgrade Instructions** ..... **11**
Running in Mixed Mode ..... 12
**Getting Help with NetWitness Platform** ..... **13**
Self-Help Resources ..... 13
Contact RSA Support ..... 13
**Upgrade Tasks** ..... **14**
Important Notes - Read This First ..... 14
Synchronize Time on Component Hosts with NW Server Host ..... 14
Mixed Mode Unsupported for ESA Hosts ..... 14
Respond Server Service Not Enabled Until NW Server and Primary ESA Host Upgraded to 11.5.3.2 ..... 14
Task 1: Upgrade External Repository ..... 14
Task 2: Disable Decoder Services ..... 15
Task 3: Upgrade the Patch ..... 15
**Upgrade Options** ..... **16**
Option 1: Online Method (Connectivity to Live Services): Upgrade Using NetWitness Platform User Interface ..... 16
Prerequisites ..... 16
Procedure ..... 16

Option 2: Offline Method (No connectivity to Live Services): Upgrade using the Command Line Interface ..... 17
Download the 11.5.3.2 Patch ..... 17
Procedure ..... 18
External Repo Instructions for CLI Upgrade ..... 21
Option 3: Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface ..... 21
**Post-Upgrade Tasks ..... 22**
Post Upgrade Tasks for Customers Upgrading from version 11.5.0.0 ..... 22
Task 1 (Optional) - Move the custom certificates ..... 22
Task 2- Enable Decoder Services ..... 22
Post Upgrade Tasks for Customers Upgrading from version 11.3.x.x or 11.4.x.x ..... 22
**Build Numbers ..... 23**
**Appendix A. Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface. ..... 24**
Download the 11.5.3.2 Patch ..... 24
Upgrading from 11.3.1.x or 11.3.2.x or 11.4.1.x or 11.5.0.0 to 11.5.3.2 ..... 28
Upgrading from 11.4.0.0, or 11.4.0.1 to 11.5.3.2 ..... 28

# Introduction

This document lists the security fixes made to improve NetWitness Platform 11.5. Read this document before deploying or upgrading to NetWitness Platform 11.5.3.2.

## 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: Known Issues.

### Security Fixes

For detailed information on Security Fixes, see Security Advisories.

# What's New

The RSA NetWitness Platform 11.5.3.2 release provides new features, enhancements, and security fixes for every role in the Security Operation Center.

## Enhancements

The following sections are a complete list and description of enhancements to specific capabilities:

- Licensing and Packaging

To locate the documents referred to in this section, go to the RSA NetWitness Platform 11.x Master Table of Contents. Product Documentation has links to the documentation for this release.

## Licensing and Packaging

### Throughput License Calculation Changes

The RSA NetWitness Platform versions 11.5.1 to 11.6, includes fixes to the metrics used in reporting for Network (Packet) Throughput usage. License metrics includes the overall network traffic analyzed and the raw network data stored after the analysis. Your Network Throughput License usage may increase, which may cause license violation banners in some situations. The Out-of-Compliance notifications for Network Throughput licenses has been adjusted to delay the display of the license violation banner by 45-days. For more information, see the *Licensing Management Guide*.

# 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: Known Issues.

## Security Fixes

For more information on Security Fixes, see Security Advisories.

## Administration Fixes

| Tracking Number | Description |
|---|---|
| ASOC-109350 | When the Admin server develops a memory leak, the NetWitness UI displays *503 Service Unavailable Error* , indicating that the Admin server is temporarily unable to handle the request. |

## Malware Fixes

| Tracking Number | Description |
|---|---|
| ASOC-109566 | Malware Analytics scan jobs do not retrieve any result when you perform a manual file analysis. It displays the following error: *Communication error. Unable to process request* |

## Respond Server Fixes

| Tracking Number | Description |
|---|---|
| SACE-15428 | 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: *[ alert-processing-pipeline] ERROR RiskScoring\|No File found to calculate score for Alert : Gets Current User As SYSTEM* |

## Reporting Engine Fixes

| Tracking Number | Description |
|---|---|
| ASOC-109518 | 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. |
| ASOC-109455 | Korean characters in file names and report content are not displayed accurately. |

## Context Hub Fixes

| Tracking Number | Description |
|---|---|
| ASOC-109469 | While upgrading to 11.5.3.0, the *rsa-nw-contexthub-server service* fails. It displays the error: *Algorithm not allowable in FIPS140 mode: PBE/PKCS5/MD5/DES/CBC/64*. |
| ASOC-109825 | In the RSA NetWitness Platform UI, when you import a Context Hub list from a CSV file, the first row of the list does not appear. |
| ASOC-109483 | The context hub server displays the *Duplicate Key and Server in Unhealthy State* errors. |

## SCL Fixes

| Tracking Number | Description |
|---|---|
| ASOC-108885 | When a rollover occurs in the Log Collector, the Secure Cloud Link begins to collect information from the last session ID, instead of the first session ID. |

## ESA Fixes

| Tracking Number | Description |
|---|---|
| ASOC-110106 | The Admin server notifies errors on the ESA rules that are deployed. |

## Log Collector Fixes

| Tracking Number | Description |
|---|---|
| ASOC-109851 | Inconsistent communication between a Virtual Log Collector (VLC) and a Log Collector that is installed on a Log Decoder, causes the log files to be removed. |
| ASOC-106564 | Log collection delays in Virtual Log Collector (VLC). When you send logs to the Log Decoder and the VLC, the logs that are sent to Log Decoder are received and found on the Investigation page immediately, but there is a delay for the logs that are sent to the VLC. |

# End of Life Functionality

The following table provides information on end of life functionality and features in RSA NetWitness Platform11.5.3.2 release.

## End of Life Functionality and Features in 11.5.3.2

| Feature | Notes |
| --- | --- |
| Live Connect Data Source | Live Connect Data Source is not supported in NetWitness Platform release 11.5.3.2. |

# Upgrade Instructions

You need to read the information and follow these procedures for upgrading NetWitness Platform version 11.5.3.2.

| Upgrade Path | Action Item |
|---|---|
| From 11.3.x.x or 11.4.x.x to 11.5.3.2 | Download the following files:<br>• 11.5.0.0 base pack<br>• 11.5.1.0 service pack<br>• 11.5.2.0 service pack<br>• 11.5.3.0 service pack<br>• 11.5.3.1 patch release<br>• 11.5.3.2 patch release |
| From 11.5.0.x to 11.5.3.2 | Download the following files:<br>• 11.5.1.0 service pack<br>• 11.5.2.0 service pack<br>• 11.5.3.0 service pack<br>• 11.5.3.1 patch release<br>• 11.5.3.2 patch release |
| From 11.5.1.0 to 11.5.3.2 | Download the following files:<br>• 11.5.2.0 service pack<br>• 11.5.3.0 service pack<br>• 11.5.3.1 patch release<br>• 11.5.3.2 patch release |
| From 11.5.2.0 to 11.5.3.2 | Download the following files:<br>• 11.5.3.0 service pack<br>• 11.5.3.1 patch release<br>• 11.5.3.2 patch release |
| From 11.5.3.0 to 11.5.3.2 | Download the following files:<br>• 11.5.3.1 patch release<br>• 11.5.3.2 patch release |
| From 11.5.3.1 to 11.5.3.2 | Download the following file:<br>• 11.5.3.2 patch release |

You can upgrade 11.5.3.2 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 11.3.x.x or 11.4.x.x, see the *RSA NetWitness Platform 11.5 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.

# 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 | https://community.rsa.com<br>In the main menu, click **My Cases**. |
| International Contacts (How to Contact RSA Support) | https://community.rsa.com/docs/DOC-1294 |
| Community | https://community.rsa.com/community/support |

# 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 11.5.3.2

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 11.5.3.2. 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 11.5.3.2.

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-11.5.3.2.zip`.
   The following is the structure after upgrading the external repository:


## Task 2: Disable Decoder Services

Before upgrading to 11.5.3.2, 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

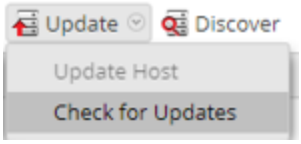
Make sure that:

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. 11.5.3.2 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 **11.5.3.2** 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 11.5.3.2, 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 11.5.3.2 Patch

Download the RSA NetWitness Platform 11.5.3.2 Upgrade Pack file, which contain all the NetWitness Platform 11.5.3.2 upgrade files, from the RSA Link https://community.rsa.com/t5/rsa-netwitness-platform/tkb-p/netwitness-downloads to a local directory.
`netwitness-11.5.3.2.zip`

| Upgrading from | Download and Stage file |
|---|---|
| 11.3.x.x | `netwitness-11.5.0.0.zip`, `netwitness-11.5.1.0.zip`, `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` |

| Upgrading from | Download and Stage file |
|---|---|
| 11.4.x.x | `netwitness-11.5.0.0.zip`, `netwitness-11.5.1.0.zip`, `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` |
| 11.5.0.0 | `netwitness-11.5.1.0.zip`, `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`,`netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` |
| 11.5.1.0 | `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`,`netwitness-11.5.3.1.zip` , and `netwitness-11.5.3.2.zip` |
| 11.5.2.0 | `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip` , and `netwitness-11.5.3.2.zip` |
| 11.5.3.0 | `netwitness-11.5.3.1.zip` and `netwitness-11.5.3.2.zip` |
| 11.5.3.1 | `netwitness-11.5.3.2.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 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 11.3.x.x or 11.4.x.x to 11.5.3.2**, you must stage 11.5.0.0, 11.5.3.1, and 11.5.3.2. Log into the `/root` directory of the NetWitness Server and create the following directories:
  `/tmp/upgrade/11.5.0.0`
  `/tmp/upgrade/11.5.1.0`
  `/tmp/upgrade/11.5.2.0`
  `/tmp/upgrade/11.5.3.0`
  `/tmp/upgrade/11.5.3.1`
  `/tmp/upgrade/11.5.3.2`
  and then copy the package zip files to the `/root` directory of the NetWitness Server and extract the package files from `/root` to the appropriate directories:
  `unzip netwitness-11.5.0.0.zip -d /tmp/upgrade/11.5.0.0`

```
unzip netwitness-11.5.1.0.zip -d /tmp/upgrade/11.5.1.0
unzip netwitness-11.5.2.0.zip -d /tmp/upgrade/11.5.2.0
unzip netwitness-11.5.3.0.zip -d /tmp/upgrade/11.5.3.0
unzip netwitness-11.5.3.1.zip -d /tmp/upgrade/11.5.3.1
unzip netwitness-11.5.3.2.zip -d /tmp/upgrade/11.5.3.2
```

- **If you are upgrading from 11.5.0.0 to 11.5.3.2**, you only need to stage 11.5.1.0, 11.5.2.0, 11.5.3.0, 11.5.3.1, and 11.5.3.2. Log into the `/root` to the directory of the NetWitness Server and create the following directory:
  ```
  /tmp/upgrade/11.5.1.0
  /tmp/upgrade/11.5.2.0
  /tmp/upgrade/11.5.3.0
  /tmp/upgrade/11.5.3.1
  /tmp/upgrade/11.5.3.2
  ```
  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/11.5.3.2` directory:
  ```
  unzip netwitness-11.5.1.0.zip -d /tmp/upgrade/11.5.1.0
  unzip netwitness-11.5.2.0.zip -d /tmp/upgrade/11.5.2.0
  unzip netwitness-11.5.3.0.zip -d /tmp/upgrade/11.5.3.0
  unzip netwitness-11.5.3.1.zip -d /tmp/upgrade/11.5.3.1
  unzip netwitness-11.5.3.2.zip -d /tmp/upgrade/11.5.3.2
  ```
- **If you are upgrading from 11.5.1.0 to 11.5.3.2**, you only need to stage 11.5.2.0, 11.5.3.0, 11.5.3.1, and 11.5.3.2. Log into the `/root` to the directory of the NetWitness Server and create the following directory:
  ```
  /tmp/upgrade/11.5.2.0
  /tmp/upgrade/11.5.3.0
  /tmp/upgrade/11.5.3.1
  /tmp/upgrade/11.5.3.2
  ```
  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/11.5.3.2` directory:
  ```
  unzip netwitness-11.5.2.0.zip -d /tmp/upgrade/11.5.2.0
  unzip netwitness-11.5.3.0.zip -d /tmp/upgrade/11.5.3.0
  unzip netwitness-11.5.3.1.zip -d /tmp/upgrade/11.5.3.1
  unzip netwitness-11.5.3.2.zip -d /tmp/upgrade/11.5.3.2
  ```
- **If you are upgrading from 11.5.2.0 to 11.5.3.2**, you only need to stage 11.5.3.0, 11.5.3.1, and 11.5.3.2. Log into the `/root` to the directory of the NetWitness Server and create the following directory:
  ```
  /tmp/upgrade/11.5.3.0
  /tmp/upgrade/11.5.3.1
  /tmp/upgrade/11.5.3.2
  ```
  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/11.5.3.2` directory:
  ```
  unzip netwitness-11.5.3.0.zip -d /tmp/upgrade/11.5.3.0
  ```

```
unzip netwitness-11.5.3.1.zip -d /tmp/upgrade/11.5.3.1
unzip netwitness-11.5.3.2.zip -d /tmp/upgrade/11.5.3.2
```

- **If you are upgrading from 11.5.3.0 to 11.5.3.2**, you only need to stage 11.5.3.1 and 11.5.3.2. Log into the `/root` to the directory of the NetWitness Server and create the following directory:
  `/tmp/upgrade/11.5.3.1`
  `/tmp/upgrade/11.5.3.2`
  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/11.5.3.2` directory:
  ```
  unzip netwitness-11.5.3.1.zip -d /tmp/upgrade/11.5.3.1
  unzip netwitness-11.5.3.2.zip -d /tmp/upgrade/11.5.3.2
  ```
- **If you are upgrading from 11.5.3.1 to 11.5.3.2**, you only need to stage 11.5.3.2. Log into the `/root` to the directory of the NetWitness Server and create the following directory:
  `/tmp/upgrade/11.5.3.2`
  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/11.5.3.2` directory:
  ```
  unzip netwitness-11.5.3.2.zip -d /tmp/upgrade/11.5.3.2
  ```

**Upgrading the NetWitness Server and component hosts**

1. Initialize the upgrade, using the following command:
   ```
   upgrade-cli-client --init --version 11.5.3.2 --stage-dir /tmp/upgrade
   ```

   **Important:** Once *init* is performed, do not reboot the SA server or restart jetty.
2. Upgrade Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.5.3.2
   ```
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 Getting Help with NetWitness Platform.

## External Repo Instructions for CLI Upgrade

**Note:** The external repo should have separate directories for 11.5.0.0 and 11.5.3.2, 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 11.5.3.2 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.5.3.2` and extract the zip package.
   ```
   unzip netwitness-11.5.3.2.zip -d /tmp/upgrade/11.5.3.2
   ```
2. Initialize the upgrade, using the following command:
   ```
   upgrade-cli-client --init --version 11.5.3.2--stage-dir /tmp/upgrade
   ```
3. Upgrade Netwitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.5.3.2
   ```
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 Getting Help with NetWitness Platform.

# 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 11.5.0.0

Post Upgrade Tasks for Customers Upgrading from version 11.3.x.x or 11.4.x.x

## Post Upgrade Tasks for Customers Upgrading from version 11.5.0.0

### 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 11.5.3.2, 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 11.3.x.x or 11.4.x.x

Perform all the post upgrade tasks mentioned in *Upgrade Guide for RSA NetWitness Platform 11.5.0.0*.

# Build Numbers

The following table lists the build numbers for the components of NetWitness Platform 11.5.3.2.

| Component | Version Number |
|---|---|
| NetWitness Cloud Link Server | 11.5.3.2-210504093810.5 |
| NetWitness Config Management | 11.5.3.2-2104201919.5 |
| NetWitness Platform Admin Server | 11.5.3.2-210518040600.5 |
| NetWitness Bootstrap | 11.5.3.2-2104201914.5 |
| NetWitness Component Descriptor | 11.5.3.2-2105232222.5 |
| NetWitness Contexthub Server | 11.5.3.2-210505070122.5 |
| NetWitness Correlation Server | 11.5.3.2-210519051210.5 |
| NetWitnesss License Server | 11.5.3.2-210505055647.5 |
| NetWitness Log Collector | 11.5.3.2-14915.5 |
| NetWitness Log Collector Perl | 11.5.3.2-14915.5 |
| NetWitness Log Collector Tools | 11.5.3.2-14915.5 |
| NetWitness Deployment Upgrade | 11.5.3.2-2104201918.5 |
| NetWitness Legacy Web Server | 11.5.3.2-210512104303.5 |
| NetWitness Respond Server | 11.5.3.2-210518092931.5 |
| NetWitness UI | 11.5.3.2-210505071210.5 |
| Malware Analytics Server | 11.5.3.2-210510063324.5 |

# 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.

**Caution:** The offline User Interface method is only available if you are upgrading a host from 11.3.1.x or 11.4.1.x or 11.5.0.0 to 11.5.3.2. If you are upgrading a host on an earlier version, you must use the Appendix A. Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface. method. After you complete Step 5 in Appendix A. Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface., go to Upgrading from 11.3.1.x or 11.3.2.x or 11.4.1.x or 11.5.0.0 to 11.5.3.2

**Caution:** If you are upgrading a host from 11.4.0.x or 11.4.1.x or 11.5.0.0 to 11.5.3.2 using the offline User Interface method, in Step 5 of Appendix A. Offline Method (No connectivity to Live Services): Upgrade using the NetWitness Platform User Interface., the upgrade will fail with the message Download error. You can still complete the upgrade successfully by following the steps in Upgrading from 11.4.0.0, or 11.4.0.1 to 11.5.3.2 .

## Download the 11.5.3.2 Patch

Download the RSA NetWitness Platform 11.5.3.2 Upgrade Pack file, which contain all the RSA NetWitness Platform 11.5.3.2 upgrade files, from the RSA Link https://community.rsa.com/t5/rsa-netwitness-platform/tkb-p/netwitness-downloads to a local directory.
`netwitness-11.5.3.2.zip`

| Upgrading from | Download and Stage file |
|---|---|
| 11.3.x.x | `netwitness-11.5.0.0.zip`, `netwitness-11.5.1.0.zip`, `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` |
| 11.4.x.x | `netwitness-11.5.0.0.zip`, `netwitness-11.5.1.0.zip`, `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` |
| 11.5.0.0 | `netwitness-11.5.1.0.zip`, `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` |

| Upgrading from | Download and Stage file |
|---|---|
| 11.5.1.0 | `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`,`netwitness-11.5.3.1.zip` , and `netwitness-11.5.3.2.zip` |
| 11.5.2.0 | `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip` , and `netwitness-11.5.3.2.zip` |
| 11.5.3.0 | `netwitness-11.5.3.1.zip` and `netwitness-11.5.3.2.zip` |
| 11.5.3.1 | `netwitness-11.5.3.2.zip` |

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

- If you are upgrading from 11.3.1.0 or later to 11.5.3.2, download the `netwitness-11.5.0.0.zip`, `netwitness-11.5.1.0.zip`, `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.5.0.0 to 11.5.3.2, download the `netwitness-11.5.1.0.zip`, `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip`, upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.5.1.0 to 11.5.3.2, download the `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip`, upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.5.2.0 to 11.5.3.2, download the `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip`, upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.5.3.0 to 11.5.3.2, download the `netwitness-11.5.3.1.zip` and `netwitness-11.5.3.2.zip`, upgrade package from RSA Link to a local directory.
- If you are upgrading from 11.5.3.1 to 11.5.3.2, download the `netwitness-11.5.3.2.zip`, upgrade package from RSA Link to a local directory.

1. SSH to the NW Server host.
2. If you are upgrading from 11.3.1.0 or later to 11.5.3.2, copy `netwitness-11.5.0.0.zip`, `netwitness-11.5.1.0.zip`, `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` from the local directory to the `/var/lib/netwitness/common/update-stage/` staging folder.

```
sudo cp /tmp/netwitness-11.5.0.0.zip /var/lib/netwitness/common/update-stage/
sudo cp /tmp/netwitness-11.5.1.0.zip /var/lib/netwitness/common/update-stage/
sudo cp /tmp/netwitness-11.5.2.0.zip /var/lib/netwitness/common/update-stage/
sudo cp /tmp/netwitness-11.5.3.0.zip /var/lib/netwitness/common/update-
```

```
stage/
sudo cp /tmp/netwitness-11.5.3.1.zip /var/lib/netwitness/common/update-
stage/
sudo cp /tmp/netwitness-11.5.3.2.zip /var/lib/netwitness/common/update-
stage/
```

3. If you are upgrading from 11.5.0.0 to 11.5.3.2, copy `netwitness-11.5.1.0.zip`, `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` from the local directory to the `/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:
   ```
   sudo cp /tmp/netwitness-11.5.1.0.zip /var/lib/netwitness/common/update-
   stage/
   sudo cp /tmp/netwitness-11.5.2.0.zip /var/lib/netwitness/common/update-
   stage/
   sudo cp /tmp/netwitness-11.5.3.0.zip /var/lib/netwitness/common/update-
   stage/
   sudo cp /tmp/netwitness-11.5.3.1.zip /var/lib/netwitness/common/update-
   stage/
   sudo cp /tmp/netwitness-11.5.3.2.zip /var/lib/netwitness/common/update-
   stage/
   ```
   NetWitness Platform unzips the file automatically.
4. If you are upgrading from 11.5.1.0 to 11.5.3.2, copy `netwitness-11.5.2.0.zip`, `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` from the local directory to the `/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:
   ```
   sudo cp /tmp/netwitness-11.5.2.0.zip /var/lib/netwitness/common/update-
   stage/
   sudo cp /tmp/netwitness-11.5.3.0.zip /var/lib/netwitness/common/update-
   stage/
   sudo cp /tmp/netwitness-11.5.3.1.zip /var/lib/netwitness/common/update-
   stage/
   sudo cp /tmp/netwitness-11.5.3.2.zip /var/lib/netwitness/common/update-
   stage/
   ```
   NetWitness Platform unzips the file automatically.
5. If you are upgrading from 11.5.2.0 to 11.5.3.2, copy `netwitness-11.5.3.0.zip`, `netwitness-11.5.3.1.zip`, and `netwitness-11.5.3.2.zip` from the local directory to the `/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:
   ```
   sudo cp /tmp/netwitness-11.5.3.0.zip /var/lib/netwitness/common/update-
   stage/
   sudo cp /tmp/netwitness-11.5.3.1.zip /var/lib/netwitness/common/update-
   stage/
   sudo cp /tmp/netwitness-11.5.3.2.zip /var/lib/netwitness/common/update-
   stage/
   ```
   NetWitness Platform unzips the file automatically.
6. If you are upgrading from 11.5.3.0 to 11.5.3.2, copy `netwitness-11.5.3.1.zip` and `netwitness-11.5.3.2.zip` from the local directory to the

`/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:

```
sudo cp /tmp/netwitness-11.5.3.1.zip /var/lib/netwitness/common/update-stage/
sudo cp /tmp/netwitness-11.5.3.2.zip /var/lib/netwitness/common/update-stage/
```

NetWitness Platform unzips the file automatically.

7. If you are upgrading from 11.5.3.1 to 11.5.3.2, copy `netwitness-11.5.3.2.zip` from the local directory to the `/var/lib/netwitness/common/upgrade-stage/` staging folder. For example:

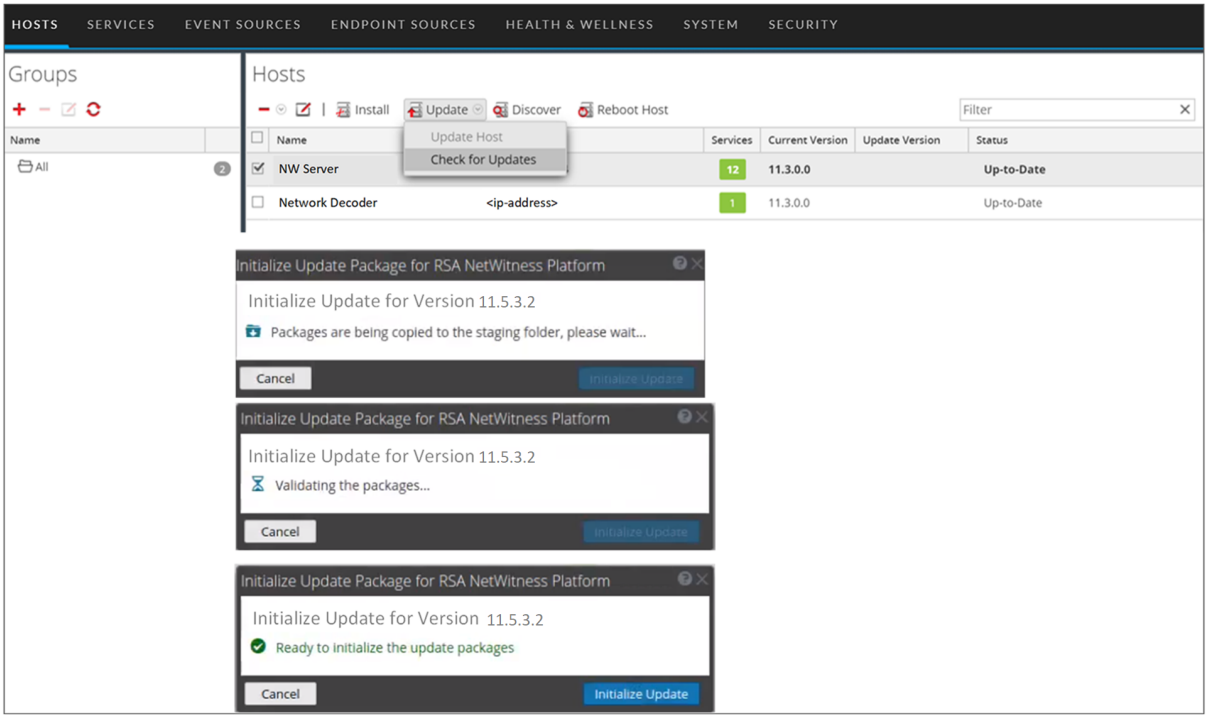
```
sudo cp /tmp/netwitness-11.5.3.2.zip /var/lib/netwitness/common/update-stage/
```

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**.

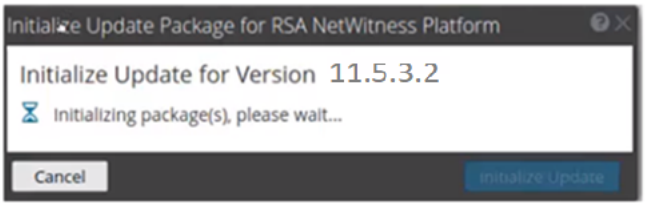
   Check for updates and wait for the update packages to be copied, validated, and ready to be initialized.
3. 


   "Ready to initialize packages" is displayed if:

   - NetWitness Platform can access the update package.
   - The package is complete and has no errors.

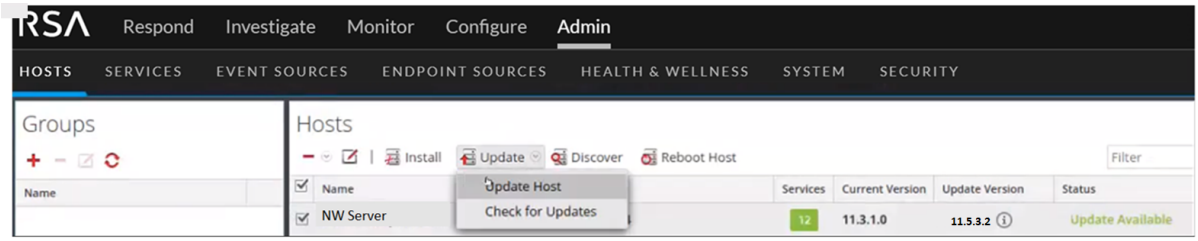
Refer to Troubleshooting Version Installations and upgrades for instructions on how to troubleshoot errors (for example, "Error deploying version <version-number>" and "Missing the following update package(s)," are displayed in the **Initiate Update Package for RSA NetWitness Platform** dialog.)

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.

## Upgrading from 11.3.1.x or 11.3.2.x or 11.4.1.x or 11.5.0.0 to 11.5.3.2

After you click **Update Hosts** in step 5, complete these steps:

1. Click **Begin Update** from the Update Available dialog.
   After the host is upgraded, it prompts you to reboot the host.
2. Click **Reboot Host** from the toolbar.

## Upgrading from 11.4.0.0, or 11.4.0.1 to 11.5.3.2

After you click **Update Hosts** in step 5, the upgrade will fail with the message Download error. You can successfully complete the upgrade by following these steps.

1. In the Command Line Interface (CLI):
   a. SSH to NW Server.
   b. Run the following command:
   ```
   upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --
   version 11.5.3.2
   ```

2. After the NW Server is successfully updated, log in to the NW Server user interface and go to  **(Admin) > Hosts**, where you are prompted to reboot the host.
3. Click **Reboot Host** from the toolbar.

You can upgrade all the other hosts directly from the user interface:

1. Click **Begin Update** from the Update Available dialog.
   After the host is upgraded, it prompts you to reboot the host.
2. Click **Reboot Host** from the toolbar.