

# NetWitness<sup>®</sup> Platform XDR

Version 11.7.2

## Upgrade Guide

## Contact Information

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

## Trademarks

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 NetWitness Community. 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.

October, 2022

# Contents

---

<b>Upgrade Overview</b>	<b>6</b>
Upgrade Paths	6
Running in Mixed Mode	6
Upgrade Considerations for ESA Hosts	7
Upgrade Considerations for STIX Custom Feeds	7
Upgrade or install Windows Legacy Collection	7
<b>Pre Upgrade Checks</b>	<b>8</b>
<b>Upgrade Preparation Tasks</b>	<b>10</b>
Task 1. (Conditional) Upgrade External Repository	10
Task 2 (Optional). Remove Legacy Package Repositories	10
Task 3. Uninstall the Security Analytics 110n language pack	10
Task 4 (Optional). Disable STIG-based FIPS Kernel Controls	11
<b>Upgrade Task</b>	<b>12</b>
Important Notes	12
Synchronize Time on Component Hosts with NW Server Host	12
Mixed Mode Unsupported for ESA Hosts	12
Respond Server Service Not Enabled Until NW Server and Primary ESA Host Upgraded to same version	13
Guidelines for Deploy_Admin Password	13
Upgrade Options for NetWitness Platform XDR	13
Option 1: Upgrade NetWitness Platform XDR	13
Option 2: Upgrade NetWitness Platform XDR Offline	15
Task 1. Populate Staging Folder (/var/lib/netwitness/common/update-stage/) with Version Upgrade Files	15
Task 2. Apply Upgrades from the Staging Area to Each Host	16
Option 3: Upgrade NetWitness Platform XDR using CLI (Offline)	17
External Repo Instructions for CLI upgrade	20
Option 4 (Optional): Pre-Stage Upgrade Repository by Downloading Packages	23
<b>Post Upgrade Tasks</b>	<b>26</b>
<b>Post Upgrade Tasks for Customers Upgrading from version 11.7.x.x</b>	<b>27</b>
General	27
(Conditional) Configure NAT-Based IP Addresses	27
(Conditional - For Warm-Standby Hosts Only) Register the Secondary IP Address of Warm-Standby Hosts	27
Review Contents of /etc/hosts.user for Obsolete Host Entries	28
Jetty Configuration	28

---

Make Sure Services Have Restarted and Are Capturing and Aggregating Data .....	28
Event Stream Analysis (ESA) .....	29
Show Updates to an ESA Rule Deployment .....	29
Respond .....	30
(Conditional) Restore Any Respond Service Custom Keys in the Aggregation Rule Schema .....	30
Reference Log Decoder .....	30
User Entity Behavior Analytics .....	30
<b>Post Upgrade Tasks for Customers Upgrading From 11.5.3.2 or 11.6.x.x .....</b>	<b>33</b>
General .....	33
(Conditional) Configure NAT-Based IP Addresses .....	33
(Conditional - For Warm-Standby Hosts Only) Register the Secondary IP Address of Warm-Standby Hosts .....	33
Review Contents of /etc/hosts.user for Obsolete Host Entries .....	34
Make Sure Services Have Restarted and Are Capturing and Aggregating Data .....	34
Event Stream Analysis (ESA) .....	35
Show Updates to an ESA Rule Deployment .....	35
Respond .....	36
(Conditional) Restore Any Respond Service Custom Keys in the Aggregation Rule Schema .....	36
Reference Log Decoder .....	36
Update UEBA Configurations .....	36
<b>Endpoint Upgrade Tasks .....</b>	<b>39</b>
Install the 11.7 or Later Relay Server .....	39
Upgrade Endpoint Agents .....	39
<b>Troubleshooting Installation and Upgrade Issues .....</b>	<b>40</b>
deploy_admin User Password Has Expired Error .....	41
Downloading Error .....	42
Error Deploying Version <version-number> Missing Update Packages .....	43
Upgrade Failed Error .....	43
External Repo Update Error .....	44
Host Update Failed Error .....	45
Missing Update Packages Error .....	46
OpenSSL 1.1.x .....	46
Patch Update to Non-NW Server Error .....	47
Reboot Host After Update from Command Line Error .....	47
Reporting Engine Restarts After Upgrade .....	47
Log Collector Service (nwlogcollector) .....	49
NW Server .....	51
Orchestration .....	52
Reporting Engine Service .....	52
Event Stream Analysis .....	52

---

ESA Troubleshooting Information .....	53
ESA Rules are Not Creating Alerts .....	53
Endpoint, UEBA, and Live Content Rules are Not Working .....	54
Example ESA Correlation Server Warning Message for Missing Meta Keys .....	55
<b>Getting Help with NetWitness Platform .....</b>	<b>56</b>
Self-Help Resources .....	56
Contact NetWitness Support .....	56
Feedback on Product Documentation .....	57

## Upgrade Overview

---

NetWitness 11.7.2.0 provides enhancements and fixes for all products in NetWitness Platform XDR. The instructions in this guide apply to both physical and virtual hosts (including AWS, Azure Public Cloud, and Google Cloud Platform) unless stated to the contrary.

## Upgrade Paths

The following upgrade paths are supported for NetWitness 11.7.2.0:

- NetWitness 11.5.3.2 to 11.7.2.0
- NetWitness 11.5.3.3 to 11.7.2.0
- NetWitness 11.6.0.0 to 11.7.2.0
- NetWitness 11.6.0.1 to 11.7.2.0
- NetWitness 11.6.1.0 to 11.7.2.0
- NetWitness 11.6.1.1 to 11.7.2.0
- NetWitness 11.6.1.2 to 11.7.2.0
- NetWitness 11.6.1.3 to 11.7.2.0
- NetWitness 11.6.1.4 to 11.7.2.0
- NetWitness 11.7.0.0 to 11.7.2.0
- NetWitness 11.7.0.1 to 11.7.2.0
- NetWitness 11.7.0.2 to 11.7.2.0
- NetWitness 11.7.1.0 to 11.7.2.0
- NetWitness 11.7.1.1 to 11.7.2.0
- NetWitness 11.7.1.2 to 11.7.2.0

## 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 *NetWitness Platform XDR 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 Considerations for ESA Hosts

Mixed mode is not supported for ESA hosts in NetWitness version 11.6 and later.

**IMPORTANT:** The NetWitness server, ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

## Upgrade Considerations for STIX Custom Feeds

The custom feeds created before version 11.6 are processed automatically. On upgrade, the data sources created for ADHOC, REST and TAXII server and the feeds are pulled automatically. See "Create a STIX Custom Feed" in the *NetWitness Platform XDR Live Service Management Guide* and "Configure STIX as a Data Source" in the *NetWitness Platform XDR Context Hub Configuration Guide* for further information.

## Upgrade or install Windows Legacy Collection

Refer to the [Windows Legacy Collection Guide for NetWitness](#)

**Note:** After you update or install Windows Legacy Collection, reboot the system to ensure that Log Collection functions correctly.

---

## Pre Upgrade Checks

---

You must run the pre-upgrade checks before you upgrade to NetWitness Platform XDR 11.7.2 to identify any issues that may result in upgrade failure.

### To run the pre-upgrade checks, perform the following:

1. Log in to Admin console.
2. Run the following command:  
`nw-precheck-tool upgrade-checklist`

The pre-upgrade checks verifies the following:

- **Security Client File Check** - Ensures `security-client-amqp.yml` file is not present.
- **Node-0 NW Service-id Status** - Ensures all the service-id is intact with all the different services in Node 0.
- **Broker Service Trustpeer Symlink** - Ensures Broker symlink file (`/etc/netwitness/ng/broker/trustpeers/`) is not broken.
- **Node-0 NW Services Status** - Checks the status of all the services in Node 0.
- **Yum External Repo Check** - Ensures external repos are not available and not enabled.
- **Node-0 RPM DB Index Check** - Checks if the RPM DB is corrupted or not.
- **Salt Master Communication** - Verifies the salt communication from Node 0 to all the Nodes.
- **Node-0 Certificates Check** - Checks if any certificates are missing, expired, or invalid issuer type.
- **Mongo Authentication** - Validates the `deploy_admin` credentials fetched from `security-cli-client` using Mongo client.
- **Rabbitmq Authentication** - Validates the `deploy_admin` credentials fetched from `security-cli-client` using RabbitMQ.
- **(Component Hosts) Node X NW Service Status** - Verifies the status of services (Active or In Active) on all the Node X.
- **(Component Hosts) Node X Certificates Check** - Checks the certificate expiry, missing, corrupted, and issuer mismatch in all categories of Node X.
- **Nodes CPU-Memory Info** - Provides CPU and Memory details of all the nodes along with the real-time available memory.
- **(Admin Server) Node 0 File System Utilization** - Verifies the disk partition utilization of `/var/netwitness/mongo`, `/var/netwitness`, and `root` on Node 0.
- **(Component Hosts) Node X File System Utilization** - Verifies the disk partition utilization of `/var/netwitness/mongo`, `/var/netwitness`, and `root` for ESA Primary and Endpoint Log Hybrid services on Node X.



- **Mongo File (ESAPrimary)** - Checks the ESA Primary node in the system or stack and verifies the permission mode of Mongo file.
- **Orchestration Server Normal Mode** - Checks if the orchestration service is running in normal or safe mode.
- **(Admin Server) Node 0 Init status** - Checks if there are any issues that might fail init process.
- **(Admin Server) Node 0 closed ports** - Checks if the service ports required for NetWitness services are open and listening on Node 0.
- **(Component Hosts) Node X closed ports** - Checks if the service ports required for NetWitness services are open and listening on Node X.
- **Fips Mode Check** - Checks to ensure that the Fips mode is disabled (set to false) before and after upgrade.
- **Node-X RPM DB Index Check** - Checks for the status of RPM DB on Node-X to make sure it is not corrupted.
- **Node-Z Yum Proxy Check** - Checks for the existence of yum.conf file and availability of proxy within the file on Node -Z.
- **Node-X Yum Proxy Check** - Checks for the existence of yum.conf file and availability of proxy within the file on Node -X.
- **Host Info Check Probe** - Checks if the required fields of information of all the hosts in the system (Host IP, Hostname, Installed Services, and Raw Version) are available.
- **Node-Z Cipher Check Probe** - Checks if the required ciphers are available in the location `/etc/rabbitmq/rabbitmq.config` on Node-0.
- **Node-X Cipher Check Probe** - Checks if the required ciphers are available in the location `/etc/rabbitmq/rabbitmq.config` on all Node-X.

---

## Upgrade Preparation Tasks

---

Complete the following tasks to prepare for the upgrade to NetWitness Platform XDR 11.7.2.0.

### Task 1. (Conditional) Upgrade External Repository

**Note:** Perform the following step only if you are using an external repository for 11.7.2.0

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

Upgrade the external repository with the latest upgrade content for the `netwitness-11.7.2.0.zip`.

For information about setting up an external repository, see "Appendix B. Set Up External Repo" in the 11.7.0.0 *Upgrade Guide for NetWitness Platform XDR*.

### Task 2 (Optional). Remove Legacy Package Repositories

Perform this task to free up space by removing unused repositories from previous releases.

1. Determine the version of the oldest NetWitness Platform host in your environment by doing one of the following:
  - Review the host list in the Admin user interface.
  - Run the following command on the NW Server:

```
upgrade-cli-client --list
```
2. You can safely remove all legacy package repository folders located at `/var/netwitness/common/repo/<version>` on the NW Server for all versions prior to the baseline major release version of the oldest active host in the environment.
  - If the oldest host version is 11.6.x.x (for example, 11.6.1.0), you can safely remove 11.0.x.x, 11.1.x.x, 11.2.x.x, 11.3.x.x, and 11.4.x.x, and 11.5.x.x repository folders. **However, do not remove repository versions greater than or equal to 11.7.0.0.**
  - If the oldest host version is 11.7.x.x, you can safely remove 11.0.x.x, 11.1.x.x, 11.2.x.x, 11.3.x.x, 11.4.x.x, 11.5.x.x, and 11.6.x.x repository folders. **However, do not remove repository versions greater than or equal to 11.7.0.0.**

### Task 3. Uninstall the Security Analytics I10n language pack

Before you upgrade from 11.5.x.x to 11.6.x.x or 11.7.x.x version, you must uninstall the Security Analytics I10n language pack.

## Task 4 (Optional). Disable STIG-based FIPS Kernel Controls

If you enabled STIG-based FIPS Kernel controls, you must disable them before initiating the NetWitness Platform XDR upgrade process to avoid boot errors. To disable STIG-based FIPS Kernel controls, run the following commands:

```
manage-stig-controls --disable-control-groups 3 --host-all  
grub2-mkconfig -o /boot/grub2/grub.cfg
```

After you upgrade NetWitness Platform XDR, ensure that you enable STIG-based FIPS Kernel controls.

**Note:** STIG-based FIPS Kernel controls which require modifications to kernel boot options are not enabled by NetWitness Platform XDR out-of-the-box.

## Upgrade Task

Upgrade the systems in your environment in the following order:

1. NW Server hosts
2. Analyst UI hosts
3. ESA Primary hosts
4. ESA Secondary hosts
5. The rest of your component hosts

**Note:** NW Server, Analyst UI, and ESA Primary and Secondary hosts must all be upgraded on the same day. The rest of your component hosts can be upgraded on the same day or later.

For information about all the host types in NetWitness, see the *Host and Services Getting Started Guide for NetWitness Platform XDR*. Go to the [NetWitness All Versions Documents](#) page and find NetWitness Platform guides to troubleshoot issues.

## Important Notes

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

Before you upgrade 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 the Admin Server host.
  - b. Run the following commands.

```
salt \* service.stop ntpd
salt \* cmd.run 'ntpdate nw-node-zero'
salt \* service.start ntpd
```

### Mixed Mode Unsupported for ESA Hosts

Mixed mode is not supported for ESA hosts in NetWitness Platform. 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 same version

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 same version. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

## Guidelines for Deploy\_Admin Password

In NetWitness Platform version 11.6 or Later, deployment account password (only on node-zero) must contain at least one number, one upper and lower case letter, and one special characters (!@#%^,+ .) along with the existing policy. The same password policy applies while updating `deploy_admin` password using `nw-manage` script.

If `deploy_admin` password is changed on Primary NW Server, it must be changed in the Warm Standby Server if it exists.

## Upgrade Options for NetWitness Platform XDR

You can choose one of the following upgrade methods based on your Internet connectivity. They are listed in the order recommended by NetWitness Platform XDR.

- [Option 1: Upgrade NetWitness Platform XDR](#)
- [Option 2: Upgrade NetWitness Platform XDR Offline](#)
- [Option 3: Upgrade NetWitness Platform XDR using CLI \(Offline\)](#)
- [Option 4 \(Optional\): Pre-Stage Upgrade Repository by Downloading Packages](#)


The following rules apply when you are upgrading hosts for all of these upgrade methods:


- You must upgrade the NW Server host first.
- You can only apply a version that is compatible with the existing host version.
- The NW Server, ESA primary, ESA secondary, and Analyst UI hosts must all be on the same NetWitness Platform version.

## Option 1: Upgrade NetWitness Platform XDR


You can use this method if the NW Server host is connected to Live Services and if you are able to obtain the package.

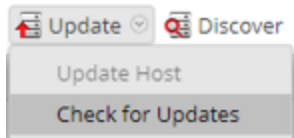
### Prerequisites

1. The **Automatically download information about new upgrades every day** option is selected and is applied in  (Admin) > System > Updates.


2. Updates are available. Go to  (Admin) > Hosts > Update > Check for Updates to check for updates. The Host view displays the **Update Available** status.
3. 11.7.2.0 is available in the **Update Version** column.

#### To upgrade from 11.5.x.x, 11.6.x.x, and 11.7.0.x to 11.7.2.0:

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




**Note:** On clicking **Check for Updates**, if you encounter the **Unauthorized** error message, follow the workaround provided in the **Host Update Failed Error** section in [Troubleshooting Installation and Upgrade Issues](#).

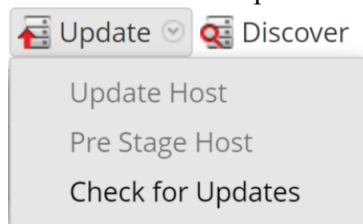
4. **Update Available** is displayed in the **Status** column if you have a version update in your Local Update Repository for the selected host.
5. Select **11.7.2.0** from the **Update Version** column. If you:
  - Want to view a dialog with the major features in the upgrade and information on the 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 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 **Reboot Host**.
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 NW Server host. All ESA, Endpoint, and Malware Analysis hosts should be upgraded to the same version as that of the NW Server host.

#### To upgrade from 11.7.1.0, 11.7.1.1, and 11.7.1.2 to 11.7.2.0:

1. Go to  (Admin) > Hosts.
2. Select the NW 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 **11.7.2.0** 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 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 **Reboot Host**.
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 NW Server host. All ESA, Endpoint, and Malware Analysis hosts should be upgraded to the same version as that of the NW Server host.

## Option 2: Upgrade NetWitness Platform XDR Offline

### Task 1. Populate Staging Folder (`/var/lib/netwitness/common/update-stage/`) with Version Upgrade Files

1. Make sure that you have downloaded the following file from NetWitness Community (<https://community.netwitness.com/>) > **Products** > **NetWitness Platform** > **Downloads** to a local directory:
  - If you are upgrading from 11.5.3.2, 11.5.3.3, 11.6.0.0, 11.6.0.1, 11.6.1.0, 11.6.1.1, 11.6.1.2, 11.6.1.3, or 11.6.1.4, download `netwitness-11.7.0.0.zip`, `netwitness-11.7.1.0.zip`, and `netwitness-11.7.2.0.zip`
  - If you are upgrading from 11.7.0.0, 11.7.0.1, or 11.7.0.2, download `netwitness-11.7.1.0.zip` and `netwitness-11.7.2.0.zip`
  - If you are upgrading from 11.7.1.0, 11.7.1.1, or 11.7.1.2, download `netwitness-11.7.2.0.zip`

- SSH to the NW Server host.
- Copy `netwitness-11.7.2.0.zip`, `netwitness-11.7.1.0.zip`, and `netwitness-11.7.0.0.zip` (if upgrading from 11.5.3.2, 11.5.3.3, 11.6.0.0, 11.6.0.1, 11.6.1.0, 11.6.1.1, 11.6.1.2, 11.6.1.3, or 11.6.1.4) from the local directory to the `/var/lib/netwitness/common/update-stage/ staging` folder.

For example:

If you are logged as a root user you can run the following command without `sudo`:

```
cp /tmp/netwitness-11.7.2.0.zip /var/lib/netwitness/common/update-stage/
```

**Note:** NetWitness Platform unzips the file automatically.

- Copy `netwitness-11.7.2.0.zip` and `netwitness-11.7.1.0.zip` (if upgrading from 11.7.0.0, 11.7.0.1, or 11.7.0.2) from the local directory to the `/var/lib/netwitness/common/update-stage/ staging` folder.

For example:

If you are logged as a root user you can run the following command without `sudo`:

```
cp /tmp/netwitness-11.7.2.0.zip /var/lib/netwitness/common/update-stage/
```

**Note:** NetWitness Platform unzips the file automatically.

- Copy `netwitness-11.7.2.0.zip` (if upgrading from 11.7.1.0, 11.7.1.1, or 11.7.1.2) from the local directory to the `/var/lib/netwitness/common/update-stage/ staging` folder.

For example:

If you are logged as a root user you can run the following command without `sudo`:


```
cp /tmp/netwitness-11.7.2.0.zip /var/lib/netwitness/common/update-stage/
```

**Note:** NetWitness Platform unzips the file automatically.

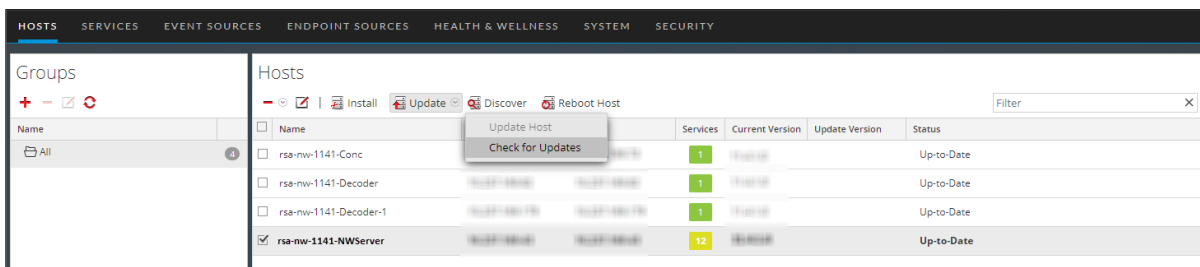
## Task 2. Apply Upgrades from the Staging Area to Each Host

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

**Note:** Optionally, you can follow the instructions provided in the [Option 4 \(Optional\): Pre-Stage Upgrade Repository by Downloading Packages](#) if you are upgrading from 11.7.1.0, 11.7.1.1, and 11.7.1.2 to 11.7.2.0.

- Log in to NetWitness.
- Go to  (Admin) > Hosts.
- Check for updates and wait for the upgrade packages to be copied, validated, and ready to be initialized.





"Ready to initialize packages" is displayed if:

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

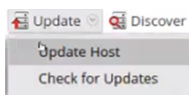
Refer to [Troubleshooting Version Installations and Updates](#) for instructions on how to troubleshoot errors (for example, "Error deploying version <version-number>" and "Missing the following update package(s)," are displayed in the **Initiate Update Package for RSA NetWitness Platform** dialog.)

#### 4. Click **Initialize Update**.

It takes some time to initialize the packages because the files are large and need to be unzipped. The time varies depending on how the host is configured.

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 upgrade 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 Host** from the toolbar.

## Option 3: Upgrade NetWitness Platform XDR using CLI (Offline)

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

### Prerequisites

Make sure that you have downloaded the following file from NetWitness Community (<https://community.netwitness.com/>) > **Products** > **NetWitness Platform** > **Downloads** to a local directory:

- If you are upgrading from 11.5.3.2, 11.5.3.3, 11.6.0.0, 11.6.0.1, 11.6.1.0, 11.6.1.1, 11.6.1.2, 11.6.1.3, or 11.6.1.4 to 11.7.2.0, download:
  - netwitness-11.7.0.0.zip
  - netwitness-11.7.1.0.zip
  - netwitness-11.7.2.0.zip

- If you are upgrading from 11.7.0.0, 11.7.0.1, or 11.7.0.2 to 11.7.2.0, download:  
netwitness-11.7.1.0.zip  
netwitness-11.7.2.0.zip
- If you are upgrading from 11.7.1.0, 11.7.1.1, or 11.7.1.2 to 11.7.2.0, download:  
netwitness-11.7.2.0.zip
- If you are using external repository, you can update the external repository with the latest upgrade content. For more information, see [External Repo Instructions for CLI upgrade](#).

## Procedure

You must perform the upgrade steps for NW Server hosts and for component servers.

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

1. Stage the 11.7.2.0 files to prepare them for the upgrade.
  - **If you are upgrading from 11.5.3.2, 11.5.3.3, 11.6.0.0, 11.6.0.1, 11.6.1.0, 11.6.1.1, 11.6.1.2, 11.6.1.3, or 11.6.1.4**, you must stage 11.7.0.0, 11.7.1.0, and 11.7.2.0. Log into the NW Server as `root` and create the following directories:  

```

/tmp/upgrade/11.7.0.0
/tmp/upgrade/11.7.1.0

/tmp/upgrade/11.7.2.0

```

 and then copy the package zip files to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directories using the following commands:  

```

unzip netwitness-11.7.0.0.zip -d /tmp/upgrade/11.7.0.0
unzip netwitness-11.7.1.0.zip -d /tmp/upgrade/11.7.1.0

unzip netwitness-11.7.2.0.zip -d /tmp/upgrade/11.7.2.0

```
  - **If you are upgrading from 11.7.0.0, 11.7.0.1, or 11.7.0.2**, you must stage 11.7.1.0 and 11.7.2.0. Log into the NW Server as `root` and create the following directory:
    - **Option 1 (Manual)** : Log into the `/root` to the directory of the NetWitness Server and create the following directory:  

```

/tmp/upgrade/11.7.1.0

/tmp/upgrade/11.7.2.0

```

 and then copy the package zip file to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directory using the following command:  

```

unzip netwitness-11.7.1.0.zip -d /tmp/upgrade/11.7.1.0

unzip netwitness-11.7.2.0.zip -d /tmp/upgrade/11.7.2.0

```

 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.
    - **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 11.7.1.0 and 11.7.2.0 package zip files to the `/root/NW` directory of the NetWitness Server.  
 After this, run the below command to extract, validate, and initialize the 11.7.2.0 zip files:  

```

[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --

```

```
download-path <download file path> --version 11.7.2.0
```

Here, <download file path> is the location where you need to copy the netwitness-11.7.1.0.zip and netwitness-11.7.2.0.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 11.7.2.0

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 11.7.2.0 again to stage 11.7.2.0.

**IMPORTANT:** After staging 11.7.2.0 (using the Option 2), if the initialization fails, run the command upgrade-cli-client --init --version 11.7.2.0 --stage-dir /tmp/upgrade. If the initialization succeeds, ignore the [step 2 Initialize the upgrade](#) and proceed with the further steps in it.

- **If you are upgrading from 11.7.1.0, 11.7.1.1, or 11.7.1.2**, you only need to stage 11.7.2.0. Log into the NW Server as root and create the following directory:
  - **Option 1 (Manual)** : Log into the /root to the directory of the NetWitness Server and create the following directory:

```
/tmp/upgrade/11.7.2.0
```

and then copy the package zip file to the /root directory of the NW Server and extract the package files from /root to the appropriate directory using the following command:

```
unzip netwitness-11.7.2.0.zip -d /tmp/upgrade/11.7.2.0
```

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.
  - **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 11.7.2.0 package zip files to the /root/NW directory of the NetWitness Server.

After this, run the below command to extract, validate, and initialize the 11.7.2.0 zip files:  
[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --download-path <download file path> --version 11.7.2.0

Here, <download file path> is the location where you need to copy the netwitness-11.7.2.0.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 11.7.2.0Once 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 11.7.2.0` again to stage 11.7.2.0.

**IMPORTANT:** After staging 11.7.2.0 (using the Option 2), if the initialization fails, run the command `upgrade-cli-client --init --version 11.7.2.0 --stage-dir /tmp/upgrade`. If the initialization succeeds, ignore the [step 2 Initialize the upgrade](#) and proceed with the further steps in it.

2. Initialize the upgrade using the following command:  
`upgrade-cli-client --init --version 11.7.2.0 --stage-dir /tmp/upgrade`
3. Upgrade the NW Server host, using the following command:  
`upgrade-cli-client --upgrade --host-key <ID / display name / (hostname/ IP address)> --version 11.7.2.0`
4. When the NW Server host upgrade is successful, reboot the host from NetWitness Platform user interface in the Hosts view.
5. (Conditional) If Warm Standby Server is deployed, repeat steps 1 to 4 on the Warm Standby Server host.
6. 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 the NW Server host. If you want to view the help content of `upgrade-cli-client`, use the command `upgrade-cli-client --help`.

**Note:** If the following error is displayed 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 service pack will install correctly. No action is required. If you encounter additional errors when updating a host to a new version, contact [Customer Support](#) for assistance.

## External Repo Instructions for CLI upgrade

For information about setting up an external repository, see "Appendix B. Set Up External Repo" in the *11.7 Upgrade Guide for NetWitness Platform XDR*. The following instructions assume that you already have an external repository set up. Go to the [NetWitness All Versions Documents](#) page and find NetWitness Platform guides to troubleshoot issues.

## 1. Stage the 11.7.2.0 files to prepare them for the upgrade.

- **If you are upgrading from 11.5.3.2, 11.5.3.3, 11.6.0.0, 11.6.0.1, 11.6.1.0, 11.6.1.1, 11.6.1.2, 11.6.1.3, or 11.6.1.4**, you must stage 11.7.0.0, 11.7.1.0, and 11.7.2.0. Log into the NW Server as `root` and create the following directories:

```
/tmp/upgrade/11.7.0.0  
/tmp/upgrade/11.7.1.0
```

```
/tmp/upgrade/11.7.2.0
```

and then copy the package zip files to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directories using the following commands:

```
unzip netwitness-11.7.0.0.zip -d /tmp/upgrade/11.7.0.0  
unzip netwitness-11.7.1.0.zip -d /tmp/upgrade/11.7.1.0
```

```
unzip netwitness-11.7.2.0.zip -d /tmp/upgrade/11.7.2.0
```

- **If you are upgrading from 11.7.0.0, 11.7.0.1, or 11.7.0.2**, you must stage 11.7.1.0 and 11.7.2.0. Log into the NW Server as `root` and create the following directory:

- **Option 1 (Manual)** : Log into the `/root` to the directory of the NetWitness Server and create the following directory:

```
/tmp/upgrade/11.7.1.0
```

```
/tmp/upgrade/11.7.2.0
```

and then copy the package zip file to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directory using the following command:

```
unzip netwitness-11.7.1.0.zip -d /tmp/upgrade/11.7.1.0
```

```
unzip netwitness-11.7.2.0.zip -d /tmp/upgrade/11.7.2.0
```

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.

- **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 11.7.1.0 and 11.7.2.0 package zip files to the `/root/NW` directory of the NetWitness Server.

After this, run the below command to extract, validate, and initialize the 11.7.2.0 zip files:

```
[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --  
download-path <download file path> --version 11.7.2.0
```

Here, `<download file path>` is the location where you need to copy the `netwitness-11.7.1.0.zip` and `netwitness-11.7.2.0.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 11.7.2.0`

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 11.7.2.0` again to stage 11.7.2.0.

**IMPORTANT:** After staging 11.7.2.0 (using the Option 2), if the initialization fails, run the command `upgrade-cli-client --init --version 11.7.2.0 --stage-dir /tmp/upgrade`. If the initialization succeeds, ignore the [step 2 Initialize the upgrade](#) and proceed with the further steps in it.

- **If you are upgrading from 11.7.1.0, 11.7.1.1, or 11.7.1.2**, you only need to stage 11.7.2.0. Log into the NW Server as `root` and create the following directory:

- **Option 1 (Manual)** : Log into the `/root` to the directory of the NetWitness Server and create the following directory:

```
/tmp/upgrade/11.7.2.0
```

and then copy the package zip file to the `/root` directory of the NW Server and extract the package files from `/root` to the appropriate directory using the following command:

```
unzip netwitness-11.7.2.0.zip -d /tmp/upgrade/11.7.2.0
```

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.

- **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 11.7.2.0 package zip files to the `/root/NW` directory of the NetWitness Server.

After this, run the below command to extract, validate, and initialize the 11.7.2.0 zip files:  
`[root@SA ~]# upgrade-cli-client --init --stage-dir /tmp/upgrade --download-path <download file path> --version 11.7.2.0`

Here, `<download file path>` is the location where you need to copy the `netwitness-11.7.2.0.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 11.7.2.0`

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 11.7.2.0` again to stage 11.7.2.0.

**IMPORTANT:** After staging 11.7.2.0 (using the Option 2), if the initialization fails, run the command `upgrade-cli-client --init --version 11.7.2.0 --stage-dir /tmp/upgrade`. If the initialization succeeds, ignore the [step 2 Initialize the upgrade](#) and proceed with the further steps in it.

2. Initialize the upgrade using the following command:  
`upgrade-cli-client --init --version 11.7.2.0 --stage-dir /tmp/upgrade`
3. Upgrade the NW Server host using the following command:  
`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version 11.7.2.0`
4. When the NW Server host upgrade is successful, reboot the host from NetWitness UI.

- (Conditional) If Warm Standby Server is deployed, repeat steps 1 to 4 on the Warm Standby Server host.
- 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 the NW Server host. If you want to view the help content of `upgrade-cli-client`, use the command `upgrade-cli-client --help`.

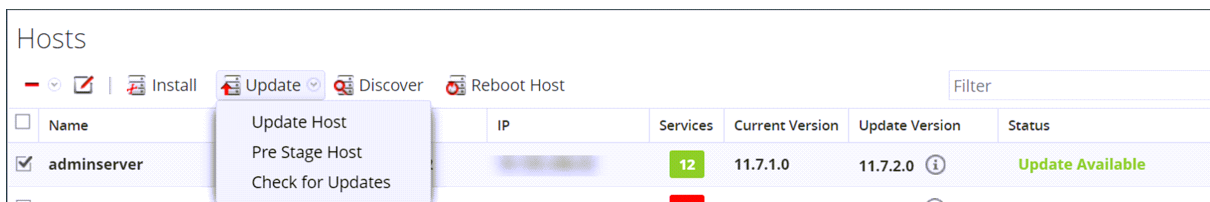
**Note:** If the following error displays during the upgrade process:  
 2017-11-02 20:13:26.580 ERROR 7994 - [ 127.0.0.1:5671]  
 o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;  
 protocol method: #method<connection.close>(reply-code=320, reply-  
 text=CONNECTION\_FORCED - broker forced connection closure with reason  
 'shutdown', class-id=0, method-id=0)  
 the service pack will install correctly. No action is required. If you encounter additional errors when updating a host to a new version, contact [Customer Support](#) for assistance.

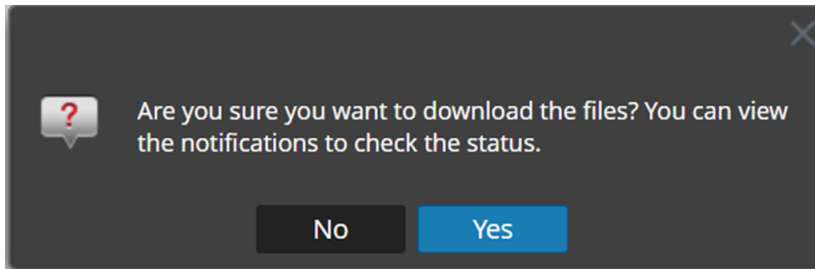
## Option 4 (Optional): Pre-Stage Upgrade Repository by Downloading Packages

You can pre-stage the upgrade repository by downloading the required packages (.zip) without affecting the system. This minimizes the upgrade downtime and ensures the upgrade is completed within the planned time.

### Procedure

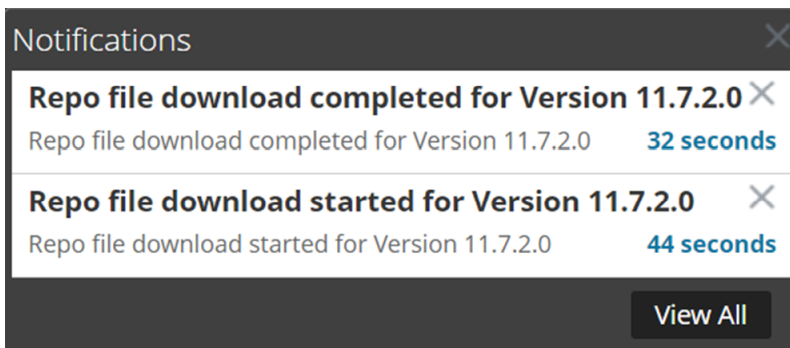
- Go to  (Admin) > **Hosts**.
- Click **Update > Check for Updates** from the toolbar.  
 All possible update versions will be displayed in the Versions drop-down list.
- Click **Update > Pre Stage Host** and select the version in the update version column.  
 A confirmation message for downloading the files is displayed.





4. Click **Yes** to download the upgrade packages to the repo.
5. Verify the status of the download in the notifications tray as shown below.

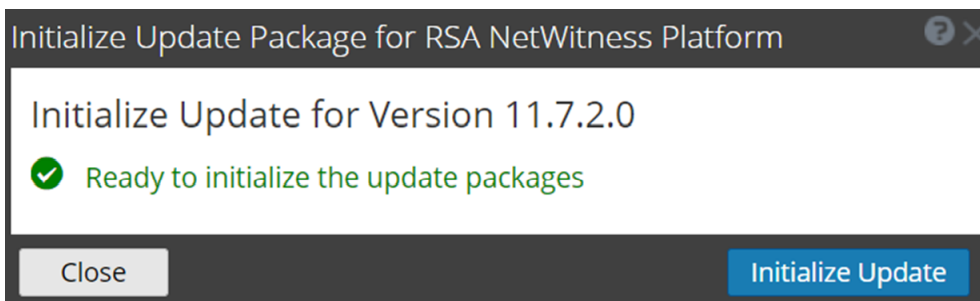
The **Pre Stage Host** and **Upgrade Host** will be disabled until pre stage is completed.



**Note:** The current version and the update version in the UI will be the same during the pre stage as it is not the actual update. This is because only the repo files are downloaded and no actual upgrade is done. The version will change only after upgrade.

6. If the download is successful, **Check for Updates** again to start the initialization.
7. Click **Initialize Update**.

The initialization of the package will take some time as the files are large and will need to be unzipped.



**IMPORTANT:** Pre Stage Repo preparation steps from 1 to 4 can be performed at any time. However, from steps 5 to 8 the upgrade process begins and you must NOT reboot the host or restart the jetty server during this time as it will corrupt the .ZIP files.

8. Check the status of initialization in the notifications tray.
9. After the initialization is completed successfully, click **Update > Update Host**.



After the host is updated, you will be prompted to reboot the host.

10. Set up the host and reboot the host.

## Post Upgrade Tasks

---

This topic is divided into two sections. Complete the tasks in one of the following sections based on your upgrade path:

- [Post Upgrade Tasks for Customers Upgrading from version 11.7.x.x](#)
- [Post Upgrade Tasks for Customers Upgrading From 11.5.3.2 or 11.6.x.x](#)

## Post Upgrade Tasks for Customers Upgrading from version 11.7.x.x

---

Complete the tasks that apply to the hosts in your environment.

- [General](#)
- [Event Stream Analysis \(ESA\)](#)
- [Respond](#)
- [Reference Log Decoder](#)
- [User Entity Behavior Analytics](#)

### General

#### (Conditional) Configure NAT-Based IP Addresses

If you have a host, such as a VLC, that requires a NAT-based IP address in order to connect to the NW Server host, you must update the host configuration with the following steps.

1. Log in to the host that requires the use of NAT IP addresses, using the console or SSH.
2. Run the following command:  

```
nw-manage --enable-nat-usage
```
3. To set the NAT address for the NW Server:
  - a. Log into the NW Server using the console or SSH.
  - b. Run the following command:  

```
nw-manage -update-host --host-id <UUID of NW Server> --ipv4-public <NAT IP of NW Server>
```

**Note:** You can find the UUID and view the current NAT IP address of the host by running `nw-manage --list-hosts`.

#### (Conditional - For Warm-Standby Hosts Only) Register the Secondary IP Address of Warm-Standby Hosts

The Warm-Standby server must be upgraded to 11.5 or later before completing the following steps.

1. Log in to the NW Server using the console or SSH.
2. Run the following command:  

```
nw-manage --add-nws-secondary-ip --ipv4 <ip address of Warm/Standby Server>
```

**Note:** If the Warm-Standby server requires a NAT-based IP address (IPv4-public) for any host to access it during failover, the NAT IP address must also be registered by running the following command: `nw-manage --add-nws-secondary-ip --ipv4 <NAT-based IP address of Warm Standby Server>`

3. Verify the correct Warm Standby host IP address value by running the following command:

```
nw-manage --get-nws-secondary-ip
```

## Review Contents of /etc/hosts.user for Obsolete Host Entries

After upgrading the NW Server host or a component host, review the contents of the `/etc/hosts.user` file for any obsolete host entries. The `/etc/hosts.user` file contains system and user-generated entries that are not managed by NetWitness Platform. However, entries from `/etc/hosts.user` are merged with NetWitness Platform-generated host mappings to create and update `/etc/hosts`. To avoid conflicts with NetWitness Platform-generated mappings, and to avoid generating connectivity errors resulting from an IP address change, NetWitness recommends that you remove any entries in `/etc/hosts.user` that include a non-loopback IP address of a NetWitness Platform host.

After updating `/etc/hosts.user`, you must refresh the system by running the following command:

```
nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>
```

## Jetty Configuration

For Jetty Configuration and related information, see **Manage Custom Host Entries** topic in the *System Maintenance Guide*.


## Make Sure Services Have Restarted and Are Capturing and Aggregating Data


Make sure that services have restarted and are capturing data (this depends on whether or not you have auto-start enabled).

If required, restart data capture and aggregation for the following services:

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver


### To Start Network Capture:

1. In the NetWitness Platform menu, go to  (Admin) > **Services**.  
The Services view is displayed.
2. Select each **Decoder** service.


3. Under  (actions), select **View > System**.

4. In the toolbar, click  **Start Capture**

### To Start Log Capture:


1. In the NetWitness Platform menu, go to  (Admin) > **Services**.  
The Services view is displayed.

2. Select each **Log Decoder** service.

3. Under  (actions), select **View > System**.


4. In the toolbar, click  **Start Capture**


### To Start Aggregation:

1. In the NetWitness Platform menu, go to  (Admin) > **Services**.  
The Services view is displayed.

2. For each **Concentrator**, **Broker**, and **Archiver** service:

a. Select the service.

b. Under  (actions), select **View > Config**.

c. In the toolbar, click  **Start Aggregation**


## Event Stream Analysis (ESA)

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.


There are no post-upgrade tasks required for ESA. For ESA troubleshooting, see [ESA Troubleshooting Information](#).

If you want to add support for Endpoint, UEBA, and Live content rules, you must update the `multi-valued` and `single-valued` parameter meta keys on the ESA Correlation service to include all the required meta keys. It is not necessary to make these adjustments during the upgrade; you can make the adjustments later at a convenient time. For detailed information and instructions, see "Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys" in the *ESA Configuration Guide*

## Show Updates to an ESA Rule Deployment

You can view changes to an ESA rule deployment, such as adding or removing rules. When there is a change to a deployment, the update icon () appears next to the name of the deployment in the Rules tab options panel.

**To show updates to an ESA rule deployment:**

1. Go to  (Configure) > **ESA Rules**. The Rules tab is displayed.
2. In the options panel, under **Deployments** click **Show Updates** on the far right.
3. Click **Deploy Now**.

If you are unable to deploy the ESA rule, see [Known Issues](#) for the workaround.

## Respond

The Primary ESA server must be upgraded to 11.7.2.0 before you can complete these tasks.

**Note:** 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 11.7.2.0. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

## (Conditional) Restore Any Respond Service Custom Keys in the Aggregation Rule Schema

**Note:** If you did not manually customize the incident aggregation rule schema, you can skip this task.

If you added custom keys in the `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file for use in the `groupBy` clause for 11.x, modify the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file and add the custom keys from the automatic backup file.

The backup file is located in `/var/lib/netwitness/respond-server/data` and it is in the following format:  
`aggregation_rule_schema.json.bak-<time of the backup>`

## Reference Log Decoder

Make sure your reference Log Decoder is upgraded to 11.5 or later versions. If you never set up a reference Log Decoder, no action is required. For details, see the *Log Parser Customization Guide*.

## User Entity Behavior Analytics

**IMPORTANT:** Before the upgrade, if you encountered and resolved the task failure issues, then after the upgrade, you must replace the `authentication.json` file before you run the post-upgrade tasks. The task failure issues in Airflow and their solutions are described in the 'Troubleshooting' topic of the *UEBA Configuration Guide*.

**IMPORTANT:** Every UEBA deployment when upgraded requires additional steps to complete the upgrade process. When you upgrade from 11.5.x to 11.5.x.x or 11.6.x to 11.6.x.x, you must follow UEBA instructions in the Upgrade Guide for 11.5.x.x or 11.6.x.x, before you upgrade to 11.7.x.

- (For Virtual Machines Only) Update the airflow parallelism on VM.  
If the UEBA system is running on VM, update the airflow parallelism to be 64 by running the following command as root from the UEBA host.

```
sed -i "s|parallelism = 256|parallelism = 64|g"
/var/netwitness/presidio/airflow/airflow.cfg
```

**Note:** Copy this command in a single line.

- Update the UEBA configuration using the following command from the UEBA machine.

```
source /etc/sysconfig/airflow

source $AIRFLOW_VENV/bin/activate

OWB_ALLOW_NON_FIPS=on python
/var/netwitness/presidio/airflow/venv/lib/python2.7/site-packages/presidio_workflows-1.0-py2.7.egg/presidio/resources/rerun_ueba_server_config.py
```

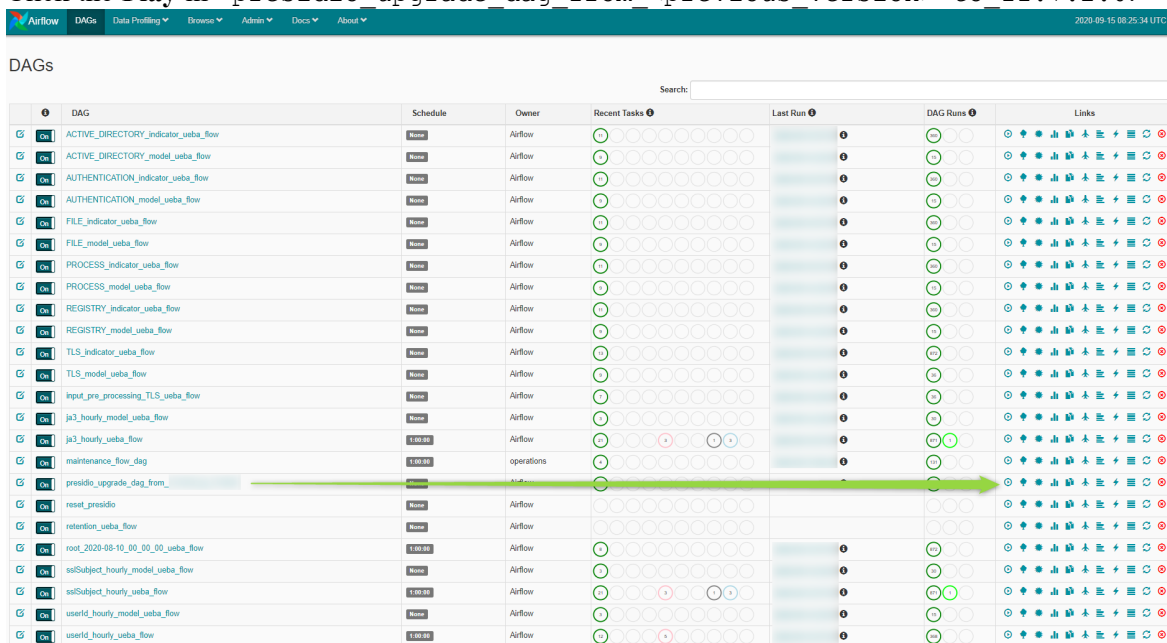
- (Optional) Update the UEBA processing schema, if needed.

NetWitness recommends that the UEBA start date is set to 28 days earlier than the current date. For UEBA systems that intend to process TLS data, you must make sure that the start date is set to no later than 14 days earlier than the current date.

For more information, see the "reset-presidio script" section in the *UEBA Configuration Guide*.

- Run the airflow upgrade DAG.

- Go to Airflow main page <https://<UEBA-host-name>/admin>
- Enter the admin username and password.
- Click the **Play** in presidio upgrade dag from <previous version> to 11.7.2.0.







## Post Upgrade Tasks for Customers Upgrading From 11.5.3.2 or 11.6.x.x

---

Complete the tasks that apply to the hosts in your environment.

- [General](#)
- [Event Stream Analysis \(ESA\)](#)
- [Respond](#)
- [Reference Log Decoder](#)
- [Update UEBA Configurations](#)

### General

#### (Conditional) Configure NAT-Based IP Addresses

If you have a host, such as a VLC, that requires a NAT-based IP address in order to connect to the NW Server host, you must update the host configuration with the following steps.

1. Log in to the host that requires the use of NAT IP addresses, using the console or SSH.
2. Run the following command:  

```
nw-manage --enable-nat-usage
```
3. To set the NAT address for the NW Server:
  - a. Log into the NW Server using the console or SSH.
  - b. Run the following command:  

```
nw-manage -update-host --host-id <UUID of NW Server> --ipv4-public <NAT IP of NW Server>
```

**Note:** You can find the UUID and view the current NAT IP address of the host by running `nw-manage --list-hosts`.

#### (Conditional - For Warm-Standby Hosts Only) Register the Secondary IP Address of Warm-Standby Hosts

The Warm-Standby server must be upgraded to 11.5 or later before completing the following steps.

1. Log in to the NW Server using the console or SSH.
2. Run the following command:  

```
nw-manage --add-nws-secondary-ip --ipv4 <ip address of Warm/Standby Server>
```

**Note:** If the Warm-Standby server requires a NAT-based IP address (IPv4-public) for any host to access it during failover, the NAT IP address must also be registered by running the following command: `nw-manage --add-nws-secondary-ip --ipv4 <NAT-based IP address of Warm Standby Server>`

3. Verify the correct Warm Standby host IP address value by running the following command:

```
nw-manage --get-nws-secondary-ip
```

## Review Contents of /etc/hosts.user for Obsolete Host Entries

After upgrading the NW Server host or a component host, review the contents of the `/etc/hosts.user` file for any obsolete host entries. The `/etc/hosts.user` file contains system and user-generated entries that are not managed by NetWitness Platform. However, entries from `/etc/hosts.user` are merged with NetWitness Platform-generated host mappings to create and update `/etc/hosts`. To avoid conflicts with NetWitness Platform-generated mappings, and to avoid generating connectivity errors resulting from an IP address change, NetWitness recommends that you remove any entries in `/etc/hosts.user` that include a non-loopback IP address of a NetWitness Platform host.

After updating `/etc/hosts.user`, you must refresh the system by running the following command:

```
nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>
```




## Make Sure Services Have Restarted and Are Capturing and Aggregating Data

Make sure that services have restarted and are capturing data (this depends on whether or not you have auto-start enabled).




If required, restart data capture and aggregation for the following services:

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver




### To Start Network Capture:

1. In the NetWitness Platform menu, go to  (Admin) > **Services**. The Services view is displayed.
2. Select each **Decoder** service.
3. Under  (actions), select **View > System**.
4. In the toolbar, click  **Start Capture**

### To Start Log Capture:

1. In the NetWitness Platform menu, go to  (Admin) > **Services**.  
The Services view is displayed.
2. Select each **Log Decoder** service.
3. Under  (actions), select **View > System**.
4. In the toolbar, click  **Start Capture**

### To Start Aggregation:

1. In the NetWitness Platform menu, go to  (Admin) > **Services**.  
The Services view is displayed.
2. For each **Concentrator**, **Broker**, and **Archiver** service:
  - a. Select the service.
  - b. Under  (actions), select **View > Config**.
  - c. In the toolbar, click  **Start Aggregation**


## Event Stream Analysis (ESA)

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.


There are no post-upgrade tasks required for ESA. For ESA troubleshooting, see [ESA Troubleshooting Information](#).

If you want to add support for Endpoint, UEBA, and Live content rules, you must update the `multi-valued` and `single-valued` parameter meta keys on the ESA Correlation service to include all the required meta keys. It is not necessary to make these adjustments during the upgrade; you can make the adjustments later at a convenient time. For detailed information and instructions, see "Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys" in the *ESA Configuration Guide*

## Show Updates to an ESA Rule Deployment

You can view changes to an ESA rule deployment, such as adding or removing rules. When there is a change to a deployment, the update icon () appears next to the name of the deployment in the Rules tab options panel.

### To show updates to an ESA rule deployment:

1. Go to  (Configure) > ESA Rules. The Rules tab is displayed.
2. In the options panel, under **Deployments** click **Show Updates** on the far right.
3. Click **Deploy Now**.

If you are unable to deploy the ESA rule, see [Known Issues](#) for the workaround.

## Respond

The Primary ESA server must be upgraded to 11.7.2.0 before you can complete these tasks.

**Note:** 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 11.7.2.0. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

## (Conditional) Restore Any Respond Service Custom Keys in the Aggregation Rule Schema

**Note:** If you did not manually customize the incident aggregation rule schema, you can skip this task.

If you added custom keys in the `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file for use in the `groupBy` clause for 11.x, modify the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file and add the custom keys from the automatic backup file.

The backup file is located in `/var/lib/netwitness/respond-server/data` and it is in the following format:  
`aggregation_rule_schema.json.bak-<time of the backup>`

## Reference Log Decoder

Make sure your reference Log Decoder is upgraded to 11.5 or later versions. If you never set up a reference Log Decoder, no action is required. For details, see the *Log Parser Customization Guide*.

## Update UEBA Configurations

**IMPORTANT:** In order to complete an upgrade process, every UEBA upgrade needs to be followed by upgrade steps. In case of gradual upgrade, follow the instruction of each upgrade's guide before continuing to the next upgrade.

**Note:** The Modeled Behaviors functionality is added to UEBA in 11.5.2. For any reason if you need to disable this functionality for your organization, see "Enable or Disable the Modeled Behaviors for Users" topic in the *UEBA Configuration Guide for NetWitness Platform XDR*.

1. (For Virtual Machines Only) Update the airflow parallelism on VM.  
If the UEBA system is running on VM, update the airflow parallelism to be 64 by running the following command as root from the UEBA host.

```
sed -i "s|parallelism = 256|parallelism = 64|g"
/var/netwitness/presidio/airflow/airflow.cfg
```

2. Update the UEBA configuration using the following command as root from the UEBA machine.  
python /var/netwitness/presidio/airflow/venv/lib/python2.7/site-packages/presidio\_workflows-1.0-py2.7.egg/presidio/resources/rerun\_ueba\_server\_config.py

3. (Optional) Update the UEBA processing schema, using the following script:

```
python
/var/netwitness/presidio/airflow/venv/lib/python2.7/sitepackages/presidio_workflows-1.0-py2.7.egg/presidio/utils/airflow/reset_presidio.pys
```

NetWitness recommends that the UEBA start date is set to 28 days earlier than the current date. For UEBA systems that intend to process TLS data, you must make sure that the start date is set to no later than 14 days earlier than the current date.

For more information about the script, see "reset-presidio script" section in the *UEBA Configuration Guide for NetWitness Platform XDR*.

4. Run the airflow upgrade DAG.

**Note:** An error message may appear at the top of the Airflow home page until the post upgrade process is complete.

- a. Go to Airflow main page <https://<UEBA-host-name>/admin> and enter the credentials.  
**User:** admin  
**Password:** The environment deploy admin password.
- b. Click the **Play** in `presidio_upgrade_dag_from_<previous_version> to_11.7.2.0`.

**Note:** A light green circle will appear next to the upgrade DAG row during the upgrade. If the upgrade process is completed successfully the light green circle changes to green. If the upgrade process fails, the light green circle changes to red.

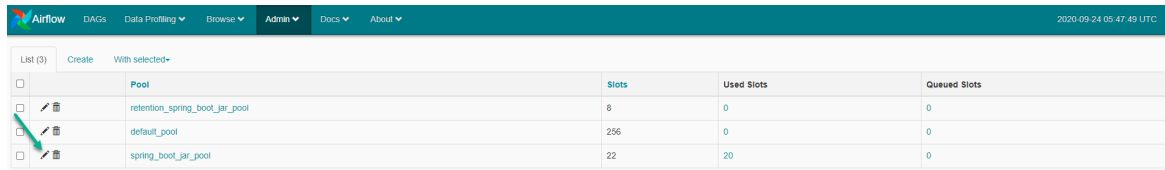
5. Set the appropriate Boot Jar Pools according to the setup.
  - **Physical Appliance:** Update the `spring_boot_jar_pool` slot value be 18.
  - **Virtual Appliance:** Update the `spring_boot_jar_pool` slot value to 22.

To update the number of Spring Boot Jar Pools:

- a. Go to the Airflow main page [https://<UEBA\\_host>/admin](https://<UEBA_host>/admin) and enter the credentials.  
**User:** admin

**Password:** The environment deploy admin password.

- b. Click the **Admin > Pools**.
- c. Edit the `spring_boot_jar_pool` and update the slots amount.



The screenshot shows the Airflow Admin interface with the 'Admin > Pools' view. The table displays the following data:

Pool	Slots	Used Slots	Queued Slots
retention_spring_boot_jar_pool	8	0	0
default_pool	256	0	0
spring_boot_jar_pool	22	20	0

## Endpoint Upgrade Tasks

---

### Install the 11.7 or Later Relay Server

If you have configured Relay Server, perform the following:

1. You must upgrade the Relay Server to 11.7 or later by downloading the Relay Server installer from the upgraded Endpoint Server. For more information see "(Optional) Installing and Configuring Relay Server" section in the *Endpoint Configuration Guide*. Go to the [NetWitness All Versions Documents](#) page and find NetWitness Platform guides to troubleshoot issues.
2. Restart the Endpoint Server using the command:

```
systemctl restart rsa-nw-endpoint-server
```

### Upgrade Endpoint Agents

See "Upgrade Agents" in the *Endpoint Agent Installation Guide for NetWitness Platform XDR* for instructions on how to upgrade agents.

## Troubleshooting Installation and Upgrade Issues

---

This section describes the error messages displayed in the Hosts view when it encounters problems updating host versions and installing services on hosts in the Hosts view. If you cannot resolve an update or installation issue using the following troubleshooting solutions, contact [Customer Support](#).

Troubleshooting instructions for the following errors that may occur during the upgrade are described in this section.

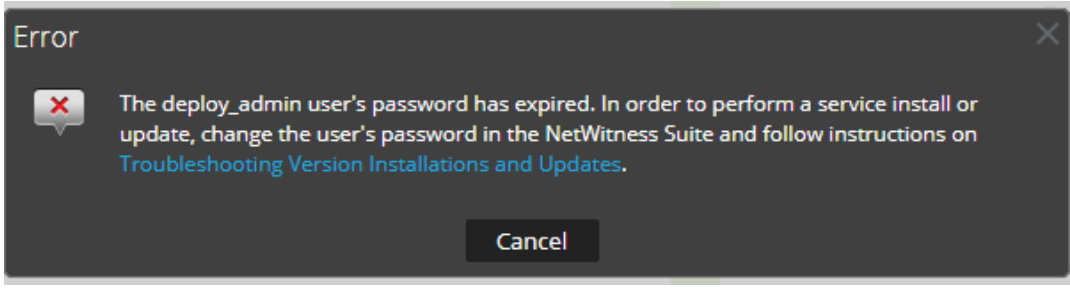
- [deploy\\_admin Password Expired Error](#)
- [Downloading Error](#)
- [Error Deploying Version <version-number> Missing Update Packages](#)
- [Upgrade Failed Error](#)
- [External Repo Update Error](#)
- [Host Update Failed Error](#)
- [Missing Update Packages Error](#)
- [OpenSSL 1.1.x Error](#)
- [Patch Update to Non-NW Server Error](#)
- [Reboot Host After Update from Command Line Error](#)
- [Reporting Engine Restarts After Upgrade](#)

Troubleshooting instructions are also provided for errors for the following hosts and services that may occur during or after an upgrade.

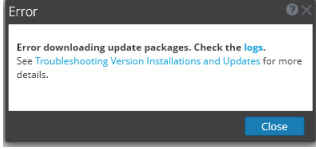

- [Log Collector Service](#)
- [NW Server](#)
- [Orchestration](#)
- [Reporting Engine](#)
- [Event Stream Analysis](#)



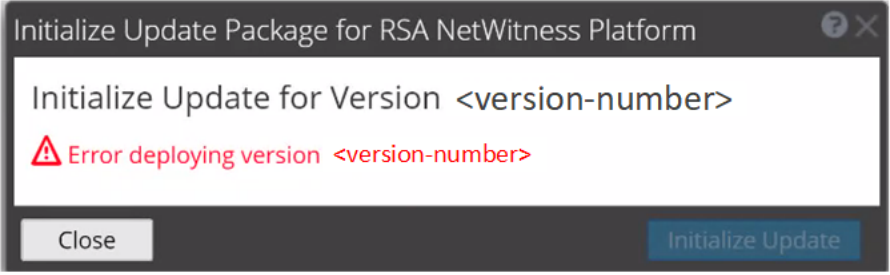
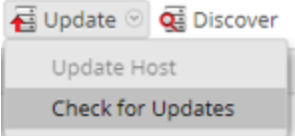
## deploy\_admin User Password Has Expired Error

<b>Error Message</b>	 An error dialog box with a dark background and a close button (X) in the top right corner. The title is "Error". The message text reads: "The deploy_admin user's password has expired. In order to perform a service install or update, change the user's password in the NetWitness Suite and follow instructions on <a href="#">Troubleshooting Version Installations and Updates</a> ." Below the message is a "Cancel" button. <p>Error</p> <p>The deploy_admin user's password has expired. In order to perform a service install or update, change the user's password in the NetWitness Suite and follow instructions on <a href="#">Troubleshooting Version Installations and Updates</a>.</p> <p>Cancel</p>
<b>Cause</b>	The deploy_admin user password has expired.
<b>Solution</b>	<p>Reset your deploy_admin password password.</p> <ol style="list-style-type: none"><li>1. On the NW Server host only, run the following command. <pre>nw-manage --update-deploy-admin-pw</pre>Please enter the new deploy_admin account password: &lt;new-deploy-admin-password&gt; Please confirm the new deploy_admin account password: &lt;new-deploy-admin-password&gt;</li><li>2. Review the output of the <code>nw-manage --update-deploy-admin-pw</code> command to verify the <code>deploy_admin</code> password was successfully updated on all hosts. If an NW host is down or fails for any reason as displayed by the output of the <code>nw-manage --update-deploy-admin-pw</code> command, run <code>nw-manage --sync-deploy-admin-pw --host-key &lt;host-identifier&gt;</code> to synchronize the password between the NW Server and the host that failed once the communication failure is resolved.</li><li>3. On the host that failed installation or orchestration, run the <code>nwsetup-tui</code> command and use the new <b>deploy_admin</b> password in response to the <b>Deployment Password</b> prompt.</li></ol>

## Downloading Error

<b>Error Message</b>	
<b>Problem</b>	When you select an update version and click <b>Update &gt;Update Host</b> , the download starts but fails to complete.
<b>Cause</b>	Version download files can be large and take a long time to download. If there are communication issues during the download it will fail.
<b>Solution</b>	<ol style="list-style-type: none"> <li>1. Try to update again.</li> <li>2. If it fails again with the same error, try to update using the offline methods as described in "Offline Method from Hosts View" or "Offline Method Using Command Line Interface" in the <i>Upgrade Guide for NetWitness Platform 11.x</i>. Go to the <a href="#">NetWitness All Versions Documents</a> page and find NetWitness Platform guides to troubleshoot issues.</li> <li>3. If you are still not able to update, contact <a href="#">Customer Support</a>.</li> </ol>
<b>Error Message</b>	If you are upgrading from NetWitness Platform 11.x.x.x to 11.6.x.x or later, offline UI upgrade fails with the <b>Download error</b> message.
<b>Solution</b>	<ol style="list-style-type: none"> <li>1. In the Command Line Interface (CLI):       <ol style="list-style-type: none"> <li>a. SSH to NW Server.</li> <li>b. Run the following command:           <pre>upgrade-cli-client --upgrade --host-key &lt;ID, IP address, hostname or display name of host&gt; --version &lt;version number&gt;</pre> <p><b>For example:</b></p> <pre>upgrade-cli-client --upgrade --host-key &lt;ID, IP address, hostname or display name of host&gt; --version 11.6.0.0</pre> </li> </ol> </li> <li>2. After the NW Server is successfully updated, log in to the NW Server user interface and go to  <b>(Admin) &gt; Hosts</b>, where you are prompted to reboot the host.</li> <li>3. Click <b>Reboot Host</b> from the toolbar.       <p>You can upgrade all the other hosts directly from the user interface:</p> <ol style="list-style-type: none"> <li>1. Click <b>Begin Update</b> from the Update Available dialog. After the host is upgraded, it prompts you to reboot the host.</li> <li>2. Click <b>Reboot Host</b> from the toolbar.</li> </ol> </li> </ol>

## Error Deploying Version <version-number> Missing Update Packages

<b>Error Message</b>	
<b>Problem</b>	<p><b>Error deploying version &lt;version-number&gt;</b> is displayed in the <b>Initialize Update Package for RSA NetWitness Platform</b> dialog after you click on <b>Initialize Update</b> if the update package is corrupted.</p>
<b>Solution</b>	<ol style="list-style-type: none"> <li>1. Click <b>Close</b> to close the dialog.</li> <li>2. Remove the version folder from staging folder.</li> <li>3. Make sure that the salt-master service is running.</li> <li>4. Recopy the update package zip file to the staging folder.</li> <li>5. In the Hosts view toolbar, select Check for Updates again.</li> </ol>  <ol style="list-style-type: none"> <li>6. Click <b>Initialize Update</b>.</li> <li>7. Click <b>Update</b> &gt; <b>Update Hosts</b> from the toolbar.</li> <li>8. Click <b>Begin Update</b> from the <b>Update Available</b> dialog. After the host is updated, it prompts you to reboot the host.</li> <li>9. Click <b>Reboot</b> from the toolbar.</li> </ol>

## Upgrade Failed Error

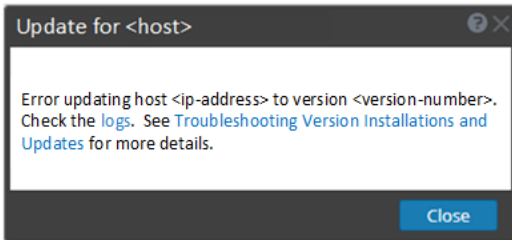
<b>Error Message</b>	<p>Received an error in the error log similar to the following when trying to update to version 11.6 or later:</p> <pre>FATAL: Chef::Exceptions::Package: yum_package[rsa-protobuffs-rt] (rsa-audit::packages line 11) had an error: Chef::Exceptions::Package: No version specified, and no candidate version available for rsa-protobuffs-rt</pre>
<b>Cause</b>	<p>Custom builds/rpms installed for certain components installed on hosts, such as in the case of installing Hotfixes.</p>

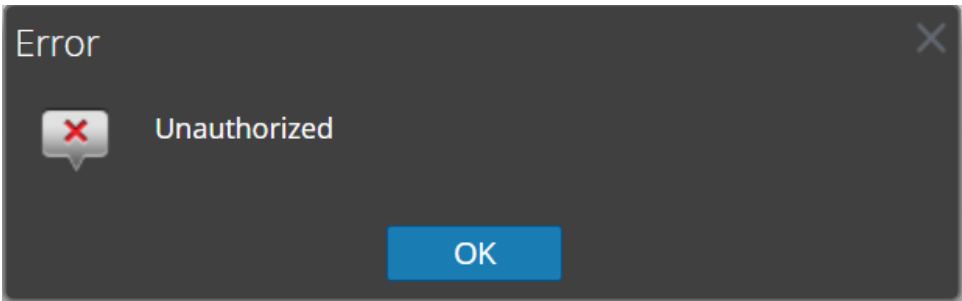

<b>Solution</b>	<p>To resolve the issue, follow the below steps.</p> <ol style="list-style-type: none"> <li>1. SSH to Admin Server.</li> <li>2. Locate the component descriptor file by running the following command.  <code>cd /etc/netwitness/component-descriptor/</code></li> <li>3. Open the component descriptor file by running the following command.  <code>vi nw-component-descriptor.json</code></li> <li>4. Search for “packages” section for the component you have custom build/rpm. For example, below shown is the package details for “concentrator” host that has custom build/rpm.  <pre> "concentrator": {   "cookbook_name": "rsa-concentrator",   "service_names": ["rsa-nw-concentrator"],   "family": "launch",   "default_port": xxxx, "description": "Concentrator",   "packages": [{ "name": "rsa-nw-concentrator",     "version" : "11.6.0.0-2003001075220.5.cecf24b.e.17.centos"   }, </pre> </li> <li>5. Delete the complete version details including (,) character in the packages section. For example, it should look like as shown below after you delete the version details.  <pre> "packages": [{   "name": "rsa-nw-concentrator" }, </pre> </li> </ol>
	<div style="border: 1px solid green; padding: 5px; background-color: #e0ffe0;"> <p><b>Note:</b> You must delete the version details for all the host that has custom builds/rpms in the component descriptor of the admin server.</p> </div> <ol style="list-style-type: none"> <li>6. Run the upgrade process again.</li> </ol>

## External Repo Update Error

<b>Error Message</b>	<p>Received an error similar to the following error when trying to update to a new version from the :</p> <pre>.Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /&lt;version-number&gt;/RSA'": URL must be http, ftp, file or https not ""</pre>
<b>Cause</b>	<p>There is an error the path you specified.</p>
<b>Solution</b>	<p>Make sure that:</p> <ul style="list-style-type: none"> <li>• the URL does exist on the NW Server host.</li> <li>• you used the correct path and remove any spaces from it.</li> </ul>

## Host Update Failed Error

<b>Error Message</b>	
<b>Problem</b>	<p>When you select an update version and click <b>Update</b> &gt; <b>Update Host</b>, the download process is successful, but the update process fails.</p>
<b>Solution</b>	<ol style="list-style-type: none"> <li>1. Try to apply the version update to the host again. Often this is all you need to do.</li> <li>2. If you still cannot apply the new version update: Monitor the following logs on NW Server as it progresses (for example, run the <code>tail -f</code> command from the command line):  <pre> /var/netwitness/uax/logs/sa.log /var/log/netwitness/orchestration-server/orchestration-server.log /var/log/netwitness/deployment-upgrade/chef-solo.log /var/log/netwitness/config-management/chef-solo.log /var/lib/netwitness/config-management/cache/chef-stacktrace.out </pre> The error appears in one or more of these logs. </li> <li>3. If you still cannot apply the update, gather the logs from step 2 and contact <a href="#">Customer Support</a>.</li> </ol>

<b>Error Message</b>	
<b>Problem</b>	<p>When you select an update version and click <b>Update</b> &gt; <b>Check for Updates</b>, the <b>Unauthorized</b> error message is displayed. As a result, the connection to the live service fails.</p>
<b>Solution</b>	<ol style="list-style-type: none"> <li>1. Make sure the Live test connection passes.</li> <li>2. Update <a href="https://update.netwitness.com/RSA-netwitness">https://update.netwitness.com/RSA-netwitness</a> in  (Admin) &gt; System &gt; Updates.</li> </ol>

	<p>3. SSH to the Admin Server and backup <code>/etc/default/jetty</code>.</p> <p>4. Update the following entry at the end of the <code>JAVA_OPTIONS</code> in the <code>/etc/default/jetty</code>.</p> <pre>JAVA_OPTIONS="\${JAVA_OPTIONS} - Drsa.nw.legacy.web.server.system.update.repo.url=https://update.netwitness.com/RSA-netwitness/ - Drsa.nw.legacy.system.update.auth.url=https://update.netwitness.com/authenticate "</pre> <p>5. Restart the jetty service. Run the following command.</p> <pre>service jetty restart</pre>
--	---

## Missing Update Packages Error

<b>Error Message</b>	<p><b>Initialize Update for Version xx.x.x.x</b>  Missing the following update package(s)  <a href="#">Download Packages from RSA Link</a></p>
<b>Problem</b>	<p><b>Missing the following update package(s)</b> is displayed in the <b>Initialize Update Package for RSA NetWitness Platform</b> dialog when you are updating a host from the <b>Hosts</b> view offline and there are packages missing in the staging folder.</p>
<b>Solution</b>	<ol style="list-style-type: none"> <li>Click <a href="#">Download Packages from NetWitness Community</a> in the <b>Initialize Update Package for RSA NetWitness Platform</b> dialog. The NetWitness Community page that contains the update files for the selected version is displayed.</li> <li>Select the missing packages from the staging folder. The <b>Initialize Update Package for RSA NetWitness Platform</b> dialog is displayed telling you that it is ready to initialize the update packages.</li> </ol>

## OpenSSL 1.1.x


<b>Error Message</b>	<p>The following example illustrates an ssh error that can occur when the ssh client is run from a host with OpenSSL 1.1.x installed:</p> <pre>\$ ssh root@10.1.2.3 ssh_dispatch_run_fatal: Connection to 10.1.2.3 port 22: message authentication code incorrect</pre>
<b>Problem</b>	<p>Advanced users who want to ssh to a NetWitness Platform host from a client that is using OpenSSL 1.1.x encounter this error because of incompatibility between CentOS 7.x and OpenSSL 1.1.x. For example:</p> <pre>\$ rpm -q openssl openssl-1.1.1-8.el8.x86_64</pre>
<b>Solution</b>	<p>Specify the compatible cipher list on the command line. For example:</p> <pre>\$ ssh -oCiphers=aes128-ctr,aes192-ctr,aes256-ctr root@10.1.2.3</pre>

```
I've read & consent to terms in IS user agreement.
root@10.1.2.3's password:
Last login: Mon Oct 21 19:03:23 2019
```

## Patch Update to Non-NW Server Error

<b>Error Message</b>	The /var/log/netwitness/orchestration-server/orchestration-server.log has an error similar to the following error: <b>API Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is not supported</b>
<b>Problem</b>	After you update the NW Server host to a version, you must update all non-NW Server hosts to the same version. For example, if you update the NW Server from 11.4.0.0 to 11.6.0.0 or later, the only update path for the non-NW Server hosts is the same version (that is, 11.6.0.0). If you try to update any non-NW Server host to a different version (for example, from 11.4.0.0 to an 11.4.x.x) you will get this error.
<b>Solution</b>	You have two options: <ul style="list-style-type: none"> <li>• Update the non-NW Server host to 11.6.0.0 or later, or</li> <li>• Do not update the non-NW Server host (keep it at its current version)</li> </ul>

## Reboot Host After Update from Command Line Error

<b>Error Message</b>	You receive a message in the User Interface to reboot the host after you update and reboot the host offline. 
<b>Cause</b>	You cannot use CLI to reboot the host. You must use the User Interface.
<b>Solution</b>	Reboot the host in the Host View in the User Interface.

## Reporting Engine Restarts After Upgrade

<b>Problem</b>	In some cases, after you upgrade to 11.6 or later from versions of 11.x, such as 11.4, the Reporting Engine service attempts to restart continuously without success.
<b>Cause</b>	The database files for live charts, alert status, or report status may not be loaded successfully as the files may be corrupted.
<b>Solution</b>	To resolve the issue, do the following: <ol style="list-style-type: none"> <li>1. Check which database files are corrupted: <p>Navigate to the file located at /var/netwitness/reserver/rsa/soc/reporting-</p> </li> </ol>

engine/logs/reporting-engine.log and check the following blocks:

- If the live charts db file is corrupted, the following logs are displayed:

```
Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception:
```

```
org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]
```

```
at org.h2.message.DbException.getJdbcSQLException(DbException.java:345)
```

```
at org.h2.message.DbException.get(DbException.java:168)
```

```
org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'chartSummaryDAOImpl': Invocation of init method failed; nested exception is com.rsa.soc.re.exception.ReportingException: java.sql.SQLException: Connections could not be acquired from the underlying database!
```

- If the alert status db file is corrupted, the following logs are displayed:

```
Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception:
```

```
org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]
```

```
at org.h2.message.DbException.getJdbcSQLException(DbException.java:345)
```

```
at org.h2.message.DbException.get(DbException.java:168)
```

```
org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertStatusHandler': Unsatisfied dependency expressed through field 'alertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertExecutionStatsDAOImpl': Unsatisfied dependency expressed through field 'persistedAlertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'persistedAlertExecutionStatsDAOImpl'
```

- If the report status db file is corrupted, the following logs are displayed:

```
org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]
```

2. To resolve the live charts database file corruption, perform the following steps:

- a. Stop the Reporting Engine service.
- b. Move the `livechart.mv.db` file from `/var/netwitness/reserver/rsa/soc/reporting-engine/livecharts` folder to a temporary location.
- c. Restart the Reporting Engine service.

**Note:** Some live charts data may be lost on performing the above steps.

To resolve the alert status or report status database file corruption, perform the following steps:

- a. Stop the Reporting Engine service.
- b. Replace the corrupted db file with the latest `alertstatusmanager.mv.db` or `reportstatusmanager.mv.db` file from `/var/netwitness/reserver/rsa/soc/reporting-engine/archives` folder.
- c. Restart the Reporting Engine service.



For more information, see the Knowledge Base article [Reporting Engine restarts After upgrade to RSA NetWitness Platform 11.4](#).

<b>Problem</b>	After you upgrade to version 11.6 or later, the Reporting Engine service does not restart.
<b>Cause</b>	The Reporting Engine service may not start due to any of the following reasons. <ul style="list-style-type: none"> <li>- workspace.xml not updated.</li> <li>- Time is not converted properly in livechart h2 database.</li> <li>- JCR (Jackrabbit repository) is corrupted with primary key violation.</li> </ul>
<b>Solution</b>	<p>To resolve the issue, run the Reporting Engine Migration Recovery tool (<code>rsa-nw-re-migration-recovery.sh</code>) on the Admin Server where the Reporting Engine service is installed.</p> <p><b>Note:</b> You can find the Reporting Engine Migration Recovery tool in the below location.  <code>/opt/rsa/soc/reporting-engine-&lt;version number&gt;-&lt;Tag&gt;/nwtools</code>  <b>For example:</b>  <code>/opt/rsa/soc/reporting-engine-11.6.0.0-&lt;Tag&gt;/nwtools</code></p> <ol style="list-style-type: none"> <li>1. SSH to Admin Server.</li> <li>2. Untar the RE (Reporting Engine) tool, run the following command.  <code>tar -xvf rsa-nw-re-recovery-tool-bundle.tar</code></li> <li>3. (Optional) If you want to untar the RE tool file in some other directory, you can create a directory and untar the RE tool. Run the following commands.  <code>mkdir &lt;NAME OF THE DIRECTORY&gt;</code>  <code>tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory &lt;PATH OF THE DIRECTORY&gt;</code></li> <li>4. Run the script, run the following command.  <code>./&lt;PATH OF THE DIRECTORY&gt;/rsa-nw-re-recovery-tool.sh</code></li> </ol> <p>For more information, see the Knowledge Base article <b>Reporting Engine Migration Recovery Tool</b>.</p>

## Log Collector Service (`nwlogcollector`)

Log Collector installation logs posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

<b>Error Message</b>	<code>&lt;timestamp&gt;.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.</code>
<b>Cause</b>	The Log Collector Lockbox failed to open after the update.
<b>Solution</b>	Log in to NetWitness and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the <i>Log Collection Configuration Guide</i> .

<b>Error Message</b>	<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found
<b>Cause</b>	The Log Collector Lockbox is not configured after the update.
<b>Solution</b>	If you use a Log Collector Lockbox, log in to NetWitness and configure the Lockbox as described in the "Configure Lockbox Security Settings" topic in the <i>Log Collection Configuration Guide</i> .

<b>Error Message</b>	<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.
<b>Cause</b>	You need to reset the stable value threshold field for the Log Collector Lockbox.
<b>Solution</b>	Log in to NetWitness and reset the stable system value password for the Lockbox as described in "Reset the Stable System Value" topic under "Configure Lockbox Security Settings" topic in the <i>Log Collection Configuration Guide</i> .

<b>Error Message</b>	<p>Decoder tries to start capture events but fails.</p> <pre style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;">Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.</pre>
<b>Solution</b>	<p>To resolve the issue, do the following steps,</p> <ol style="list-style-type: none"> <li>SSH to the Decoder host.</li> <li>Run the following commands. <pre>yum reinstall pfring* systemctl restart nwdecoder</pre> </li> </ol>

## NW Server

These logs are posted to `/var/netwitness/uax/logs/sa.log` on the NW Server Host.

<b>Problem</b>	<p>After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup;</p> <p>or,</p> <p>The following message seen in the <code>sa.log</code>.  <pre>Syslog Configuration migration failed. Restart jetty service to fix this issue</pre></p>
<b>Cause</b>	NW Server Global Audit setup migration failed to migrate from 11.4.x.x or 11.5.x.x. to 11.6.0.0 or later.
<b>Solution</b>	<ol style="list-style-type: none"> <li>SSH to the NW Server.</li> <li>Submit the following command. <pre>orchestration-cli-client --update-admin-node</pre> </li> </ol>

## Orchestration

The orchestration server logs are posted to `/var/log/netwitness/orchestration-server/orchestration-server.log` on the NW Server Host.

<b>Problem</b>	<ol style="list-style-type: none"> <li>1. Tried to upgrade a non-NW Server host and it failed.</li> <li>2. Retried the upgrade for this host and it failed again.</li> </ol>
<b>Cause</b>	<p>You will see the following message in the <code>orchestration-server.log</code>.  <code>''file' _virtual_ returned False: cannot import name HASHES''</code></p> <p>Salt minion may have been upgraded and never restarted on failed non-NW Server host</p>
<b>Solution</b>	<ol style="list-style-type: none"> <li>1. SSH to the non-NW Server host that failed to upgrade.</li> <li>2. Submit the following commands. <pre>systemctl unmask salt-minion systemctl restart salt-minion</pre> </li> <li>3. Retry the upgrade of the non-NW Server host.</li> </ol>



## Reporting Engine Service

Reporting Engine Update logs are posted to `/var/log/re_install.log` file on the host running the Reporting Engine service.

<b>Error Message</b>	<code>&lt;timestamp&gt; : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ &gt;&lt;existing-GB &gt; ] is less than the required space [ &lt;required-GB&gt; ]</code>
<b>Cause</b>	Update of the Reporting Engine failed because you do not have enough disk space.
<b>Solution</b>	Free up the disk space to accommodate the required space shown in the log message. See the "Add Additional Space for Large Reports" topic in the <i>Reporting Engine Configuration Guide</i> for instructions on how to free up disk space.

## Event Stream Analysis

<b>Problem</b>	After upgrading to version 11.6 or later, the ESA correlation server does not aggregate events from the configured data sources.
<b>Error Message</b>	Invalid username or password at <code>com.rsa.netwitness.streams.base.RecordSourceSubscription.run</code> <code>(RecordSourceSubscription.java:173)</code>
<b>Solution</b>	To resolve the issue, do the following steps. In the NetWitness user interface,

1. Go to  (**Configure**) > **ESA Rules**.  
**ESA Rules** panel is displayed with **Rules** tab open.
2. In the Rules tab options panel, under Deployments, select a deployment.
3. In the **Data Sources** section, select the data source and click  in the toolbar.
4. In the **Edit Service** dialog, type the password for that data source.
5. Click the **Test Connection** button to make sure that it can communicate with the ESA service and then click **OK**.


**Note:** Do the above procedure for all the configured data sources.

6. After you finish making changes to the deployment, click **Deploy Now** to redeploy the ESA rule deployment.

## ESA Troubleshooting Information

### ESA Rules are Not Creating Alerts


If you are not seeing any alerts, check the status of the ESA rule deployments.

1. Go to  (**Configure**) > **ESA Rules** > **Services** tab.  
The Services view is displayed, which shows the status of your ESA services and deployments.
2. In the options panel on the left, select an ESA service.
3. For each service listed, look at the deployment tabs in the panel on the right. Each tab represents a separate ESA rule deployment.
4. For each ESA rule deployment:
  - a. In the **Engine Stats** section, look at the **Events Offered** and the **Offered Rate**. They confirm that the data is being aggregated and analyzed properly. If you see 0 for Events Offered, nothing is coming in for the deployment.
  - b. In the **Rule Stats** section, look at the **Rules Enabled** and **Rules Disabled**. If there are any disabled rules, look in the **Deployed Rule Stats** section below to view the details of the disabled rules. Disabled rules show a white circle. Enabled rules show a green circle.

The screenshot displays the 'ESA - ESA Correlation' configuration page. It features several statistics sections and a table of deployed rules.

Enable	Name	Rule Type	Trial Rule	Last Detected	Events Matched	Memory Usage
<input type="checkbox"/>	No Log Traffic Detected from Device in Given Time...	Esper	No		0	0 bytes
<input type="checkbox"/>	Juniper ScreenOS Administrative Access (CVE-2015...	Esper	No	2019-12-11 22:16:19	340	0 bytes
<input type="checkbox"/>	Head Requests Flood Advanced	Esper	No		0	0 bytes
<input type="checkbox"/>	Multiple Login Failures Due to Username That Doe...	Esper	No		0	0 bytes
<input type="checkbox"/>	User Login Baseline Advanced	Esper	Yes		0	1.20 MB
<input type="checkbox"/>	Multiple Failed Logins from Multiple Diff Sources t...	Esper	No	2019-12-11 22:16:23	4080	0 bytes
<input type="checkbox"/>	RDP Inbound Traffic Advanced	Esper	No		0	0 bytes

5. If you notice any disabled rules that should be enabled:

- Go to  (Configure) > **ESA Rules** > **Rules** tab and redeploy the ESA rule deployments that contain disabled rules.
- Go back to the **Services** tab and check to see if the rules are still disabled. If the rules are still disabled, check the ESA Correlation service log files, which are located at `/var/log/netwitness/correlation-server/correlation-server.log`.

**Note:** To avoid unnecessary processing overhead, the Ignore Case option has been removed from the ESA Rule Builder - Build a Statement dialog for meta keys that do not contain text data values. During the upgrade to 11.4 or later, NetWitness Platform does not modify existing rules for the Ignore Case option. If an existing Rule Builder rule has the Ignore Case option selected for a meta key that no longer has the option available, an error occurs if you try to edit the statement and try to save it again without clearing the checkbox.

## Endpoint, UEBA, and Live Content Rules are Not Working

To support Endpoint and UEBA content as well as changes to ESA rules from Live, a data change from single-value (string) to multi-value (string array) is required for several meta keys within the ESA Correlation service. In NetWitness Platform 11.4 or later, ESA automatically adjusts the operator in the rule statement when there is a change from string to string array, but you still may need to make manual adjustments to adjust for the string array changes.

To change the string type meta keys to string array type meta keys manually in 11.4 or later, see “Configure Meta Keys as Arrays in ESA Correlation Rule Values” in the *ESA Configuration Guide*.

To use the latest Endpoint, UEBA, and Live content rules, the following default **multi-valued** meta keys are required on the ESA Correlation service in NetWitness Platform version 11.4 or later:

action , alert , alert.id , alias.host , alias.ip , alias.ipv6 , analysis.file , analysis.service , analysis.session , boc , browserprint , cert.thumbprint , checksum , checksum.all , checksum.dst , checksum.src , client.all , content , context , context.all , context.dst , context.src , dir.path , dir.path.dst , dir.path.src , directory , directory.all , directory.dst , directory.src , email , email.dst , email.src , eoc , feed.category , feed.desc , feed.name , file.cat , file.cat.dst , file.cat.src , filename.dst , filename.src , filter , function , host.all , host.dst , host.orig , host.src , host.state , inv.category , inv.context , ioc , ip.orig , ipv6.orig , netname , OS , param , param.dst , param.src , registry.key , registry.value , risk , risk.info , risk.suspicious , risk.warning , threat.category , threat.desc , threat.source , user.agent , username

The following default **single-valued** meta keys are also required on the ESA Correlation service in NetWitness Platform 11.4 or later:

accesses , context.target , file.attributes , logon.type.desc , packets

To update your meta keys, see "Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules" in the *ESA Configuration Guide*.

If you used any meta keys in the ESA rule notification templates from the Required String Array or String Meta Keys list, update the templates with the meta key changes. See "Configure Global Notification Templates" in the *System Configuration Guide*. Go to the [NetWitness All Versions Documents](#) page and find NetWitness Platform guides to troubleshoot issues.

**Note:** Advanced EPL rules may get disabled and are not automatically updated so they must be fixed manually.

For additional troubleshooting information, see "Troubleshoot ESA" in the *Alerting with ESA Correlation Rules User Guide for NetWitness Platform XDR*. Go to the [NetWitness All Versions Documents](#) page and find NetWitness Platform guides to troubleshoot issues.

## Example ESA Correlation Server Warning Message for Missing Meta Keys

If you see a warning message in the ESA Correlation server error logs that means there is a difference between the `default-multi-valued parameter` and `multi-valued parameter` meta key values, the new Endpoint, UEBA, and Live content rules will not work. Completing the "Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules" procedure in the *ESA Configuration Guide* should fix the issue.

### Multi-Valued Warning Message Example

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[alert, alert_id, browserprint, cert_thumbprint, checksum, checksum_all, checksum_dst, checksum_src, client_all, content, context, context_all, context_dst, context_src, dir_path, dir_path_dst, dir_path_src, directory, directory_all, directory_dst, directory_src, email_dst, email_src, feed_category, feed_desc, feed_name, file_cat, file_cat_dst, file_cat_src, filename_dst, filename_src, filter, function, host_all, host_dst, host_orig, host_src, host_state, ip_orig, ipv6_orig, OS, param, param_dst, param_src, registry_key, registry_value, risk, risk_info, risk_suspicious, risk_warning, threat_category, threat_desc, threat_source, user_agent] are still MISSING from multi-valued
```

### Single Value Warning Message Example

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[accesses, context_target, file_attributes, logon_type_desc, packets] are still MISSING from single-valued
```

## 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:

- See the documentation for all aspects of NetWitness here:  
<https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>
- See the NetWitness Knowledge Base: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>
- See Troubleshooting section in the guides.
- See also [NetWitness® Platform Blog Posts](#).
- If you need further assistance, contact NetWitness Support.

### Contact NetWitness Support

If you contact NetWitness Support, you should be at your computer. Be prepared to provide the following information:

- The version number of the 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.

NetWitness Community Portal	<a href="https://community.netwitness.com">https://community.netwitness.com</a> In the main menu, click <b>Support &gt; Case Portal &gt; View My Cases</b> .
International Contacts (How to Contact NetWitness Support)	<a href="https://community.netwitness.com/t5/support/ct-p/support">https://community.netwitness.com/t5/support/ct-p/support</a>
Community	<a href="https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions">https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions</a>
NW Update	<a href="https://update.netwitness.com">https://update.netwitness.com</a>
LiveUI	<a href="https://live.netwitness.com">https://live.netwitness.com</a>



## Feedback on Product Documentation

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