

# Release Notes

Published  
2024-01-02

## JSA 7.5.0 Update Package 6 SFS

---

# Table of Contents

What's New in JSA 7.5.0 Update Package 6 | 1

Installing the JSA 7.5.0 Update Package 6 Software Update | 1

Installation Wrap-up | 3

Clearing the Cache | 4

Known Issues and Limitations | 5

Resolved Issues | 6

# What's New in JSA 7.5.0 Update Package 6

The JSA Vulnerability Manager scanner is end of life (EOL) in 7.5.0 Update Package 6, and is no longer supported in any version of JSA. In JSA 7.5.0 Update Package 6 and later, you can continue to use third-party scanners with your JSA Vulnerability Manager platform, but you cannot scan within your DMZ.

## Installing the JSA 7.5.0 Update Package 6 Software Update

JSA 7.5.0 Update Package 6 resolves reported issues from users and administrators from previous JSA versions. This cumulative software update fixes known software issues in your JSA deployment. JSA software updates are installed by using an SFS file. The software update can update all appliances attached to the JSA Console.

The 7.5.0.20230519190832.sfs file can upgrade the following JSA versions to JSA 7.5.0 Update Package 6:

- JSA 7.3.2 (All versions from Fix Pack 3 to Fix Pack 7)
- JSA 7.3.3 (All versions from GA to Fix Pack 9)
- JSA 7.4.0 (All versions from GA to Fix Pack 4)
- JSA 7.4.1 (All versions from GA to Fix Pack 2)
- JSA 7.4.2 (All versions from GA to Fix Pack 3)
- JSA 7.5.0 (All versions prior to JSA 7.5.0 Update Package 6)

This document does not cover all the installation messages and requirements, such as changes to appliance memory requirements or browser requirements for JSA. For more information, see the [Juniper Secure Analytics Upgrading JSA to 7.5.0](#).

Ensure that you take the following precautions:

- Back up your data before you begin any software upgrade. For more information about backup and recovery, see the [Juniper Secure Analytics Administration Guide](#).
- To avoid access errors in your log file, close all open JSA webUI sessions.

- The software update for JSA cannot be installed on a managed host that is at a different software version from the Console. All appliances in the deployment must be at the same software revision to update the entire deployment.
- Verify that all changes are deployed on your appliances. The update cannot install on appliances that have changes that are not deployed.
- If this is a new installation, administrators must review the instructions in the [Juniper Secure Analytics Installation Guide](#).

To install the JSA 7.5.0 Update Package 6 software update:

1. Download the 7.5.0.20230519190832.sfs from the Juniper Customer Support website.  
<https://support.juniper.net/support/downloads/>
2. Using SSH, log into your system as the root user.
3. To verify you have enough space (5 GB) in **/store/tmp** for the JSA Console, type the following command:

```
df -h /tmp /storetmp /store/transient | tee diskchecks.txt
```

- Best directory option: **/storetmp**

It is available on all appliance types at all versions. In JSA 7.5.0 versions **/store/tmp** is a symlink to the **/storetmp** partition.

If the disk check command fails, retype the quotation marks from your terminal, then re-run the command. This command returns the details to both the command window and to a file on the Console named **diskchecks.txt**. Review this file to ensure that all appliances have **at minimum 5 GB of space available in a directory to copy the SFS** before attempting to move the file to a managed host. If required, free up disk space on any host that fails to have less than 5 GB available.

**NOTE:** In JSA 7.3.0 and later, an update to directory structure for STIG compliant directories reduces the size of several partitions. This can impact moving large files to JSA.

4. To create the **/media/updates** directory, type the following command:  
**mkdir -p /media/updates**
5. Using SCP, copy the files to the JSA Console to the **/storetmp** directory or a location with 5 GB of disk space.
6. Change to the directory where you copied the patch file.  
For example, **cd /storetmp**
7. Unzip the file in the **/storetmp** directory using the bunzip utility:  
**bunzip2 7.5.0.20230519190832.sfs.bz2**
8. To mount the patch file to the **/media/updates** directory, type the following command:

```
mount -o loop -t squashfs /storetmp/7.5.0.20230519190832.sfs /media/updates
```

9. To run the patch installer, type the following command:  
`/media/updates/installer`

**NOTE:** The first time that you run the software update, there might be a delay before the software update installation menu is displayed.

10. Using the patch installer, select **all**.

- The **all** option updates the software on all appliances in the following order:
  - Console
  - No order required for remaining appliances. All remaining appliances can be updated in any order the administrator requires.
- If you do not select the **all** option, you must select your console appliance.

As of the JSA 2014.6.r4 patch and later, administrators are only provided the option to update **all** or update the Console appliance. Managed hosts are not displayed in the installation menu to ensure that the console is patched first. After the console is patched, a list of managed hosts that can be updated is displayed in the installation menu. This change was made starting with the JSA 2014.6.r4 patch to ensure that the console appliance is always updated before managed hosts to prevent upgrade issues.

If administrators want to patch systems in series, they can update the console first, then copy the patch to all other appliances and run the software update installer individually on each managed host. The console must be patched before you can run the installer on managed hosts. When updating in parallel, there is no order required in how you update appliances after the console is updated.

If your Secure Shell (SSH) session is disconnected while the upgrade is in progress, the upgrade continues. When you reopen your SSH session and rerun the installer, the patch installation resumes.

## Installation Wrap-up

1. After the patch completes and you have exited the installer, type the following command:  
`umount /media/updates`
2. Clear your browser cache before logging in to the Console.

3. Delete the SFS file from all appliances.

### Results

A summary of the software update installation advises you of any managed host that were not updated. If the software update fails to update a managed host, you can copy the software update to the host and run the installation locally.

After all hosts are updated, administrators can send an email to their team to inform them that they will need to clear their browser cache before logging in to the JSA.

## Clearing the Cache

After you install the patch, you must clear your Java cache and your web browser cache before you log into the JSA appliance.

### Before you begin

Ensure that you have only one instance of your browser open. If you have multiple versions of your browser open, the cache might fail to clear.

Ensure that the Java Runtime Environment is installed on the desktop system that you use to view the user interface. You can download Java version 1.7 from the Java website: <http://java.com/>.

### About this task

If you use the Microsoft Windows 7 operating system, the Java icon is typically located under the Programs pane.

To clear the cache:

1. Clear your Java cache:

- a. On your desktop, select **Start > Control Panel**.
- b. Double-click the Java icon.
- c. In the Temporary Internet Files pane, click **View**.
- d. On the Java Cache Viewer window, select all **Deployment Editor entries**.
- e. Click the Delete icon.
- f. Click **Close**.
- g. Click **OK**.

2. Open your web browser.
3. Clear the cache of your web browser. If you use the Mozilla Firefox web browser, you must clear the cache in the Microsoft Internet Explorer and Mozilla Firefox web browsers.
4. Log in to JSA.

## Known Issues and Limitations

The known issues addressed in the JSA 7.5.0 Update Package 6 are listed below:

- An issue can occur where the Risks tab does not load as expected after an upgrade from JSA 7.5.0 Update Package 5 to JSA 7.5.0 Update Package 6.
- Upgrades to JSA 7.5.0 Update Package 5 might take an extended amount of time to complete due to glusterfs file cleanup. You must allow the upgrade to continue uninterrupted.
- After upgrading to JSA 7.5.0 Update Package 5, WinCollect 7.X agents can experience management or configuration change errors.
- It is possible for autoupdates to revert to a previous version of autoupdates after upgrading. This will cause autoupdate to not work as intended.

After you upgrade to JSA 7.5.0 or later, type the following command to check your autoupdate version:

```
/opt/qradar/bin/UpdateConfs.pl -v
```

- Docker services fail to start on JSA appliances that were originally installed at JSA release 2014.8 or earlier, then upgraded to 7.5.0 Update Package 2 Interim Fix 02 or 7.5.0 Update Package 3.

Before you upgrade to JSA 7.5.0 Update Package 2 Interim Fix 02, run the following command from the JSA Console:

```
xfs_info /store | grep ftype
```

Review the output to confirm the ftype setting. If the output setting displays "ftype=0", do not proceed with the upgrade to 7.5.0 Update Package 2 Interim Fix 02 or 7.5.0 Update Package 3.

See [KB69793](#) for additional details.

- After you install JSA 7.5.0, your applications might go down temporarily while they are being upgraded to the latest base image.
- After upgrading some apps remain in "error" state on deployments with more than 30 apps. Restart the apps by using the qappmanager: **/opt/qradar/support/qappmanager**.

- When adding a Data Node to a cluster, they must either all be encrypted, or all be unencrypted. You cannot add both encrypted and unencrypted Data Nodes to the same cluster.

## Resolved Issues

The resolved issues addressed in the JSA 7.5.0 Update Package 6 are listed below:

- The `/var/log` partition can fill up due to the `tomcat2.log` file not being rotated.
- Editing a managed host in a NAT group generates message "IP for host already exists in deployment".
- Removing a failed JSA app upgrade by using extensions management also removes the existing running installation.
- JSA patching can fail due to a free space check that fails.
- Aggregated searches are showing the wrong flag for some IP addresses.
- Overridden identity properties can fail to display as expected in the log activity tab.
- Out of memory for decapper on JSA Network Insights host can occur in advanced inspection level.
- Scheduled reports can run on raw data causing them to fail or take longer than expected to complete.
- Postgresql uninstalled after hostservices restarts on standby high availability managed host.
- Anomaly issues in 7.5.0 Update Package 2 prevent rules wizard from launching and effects offense creation.
- Truncated NVA configuration file can cause failures on deployed managed hosts.
- Applications can time out or fail to load due to `conman-mks` secret encryption performance.
- Offense emails might not send when custom properties in the `agent-config.xml` template use curly quotations.
- High availability setup can fail when primary and secondary IP addresses are too similar.
- After upgrading to JSA 7.5.0, `known_hosts` keys can be removed unexpectedly causing SSH errors.
- A user custom event property (CEP) can incorrectly display the owner as admin in the user interface.
- Copying a custom property can incorrectly assign the original CEP owner (admin) to a new user.
- QRoC SAASADMIN role unable to list all users associated with an asset.



- JSA apps fail to start or stop after editing an app host setting to disable encryption.
- Application-related issues might occur due to docker keystore error.
- Domain permission checks can impact performance in the CRE and might send events to store.
- "Exception reading CRE rules" error in rules used in cause and effect tests due to NullPointerException.
- Last 30 days in saved search AQL query is searching for information for 5 years.
- JSA namevaluepairparser can experience errors when the last value contains pair separator.
- "Top category type" dashboard can cause performance issues, leading to Tomcat (UI) instability.
- Radius authentication fails in 7.5.0 UP4 due to invalid attributes in configuration file.
- JSA Network Insights suspect content descriptions for cert flows can be "certificate invalid" if message header timestamp is invalid.
- Console configuration changes in deployment actions can cause global rule issues.
- Rule wizard interface refreshes unexpectedly when there is a valid JSA Vulnerability Manager license but no assigned JSA Vulnerability Manager component.
- Daily reports run out of schedule and can ignore the wizards settings.
- Inconsistent JSON custom property parsing for optimized payloads with double backslash characters.
- Rule changes from the console might be rejected by the managed host when IMQ message queue is full.
- JSA unparsed logs incorrectly go to the consoles SIM generic log source.
- Optimized JSON custom event properties with backslashes parse as N/A in the user interface.
- JSA upgrades to 7.5.0 Update Package 5 can take an extended amount of time to complete.
- Custom event property definition window displays empty "field type" when creating new CEP.
- File names from SMTP email traffic attachments are not reported in JSA Network Insights 7.5.0.
- Geographic data rules cause search and event pipeline issues when the location cache exceeds the spillover threshold.
- Tuning changes can slow ecs-ec components resulting in delays and events routing to storage.
- Enabled geographic data indexes can cause performance issues in JSA 7.5.0 Update Package 5.

---

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2024 Juniper Networks, Inc. All rights reserved.