

Release Notes

Published
2025-05-18

JSA 7.5.0 Update Package 10 SFS

Table of Contents

What's New in JSA 7.5.0 Update Package 10 | 1

Installing the JSA 7.5.0 Update Package 10 Software Update | 1

Installation Wrap-up | 3

Clearing the Cache | 3

Known Issues and Limitations | 4

Resolved Issues | 5

What's New in JSA 7.5.0 Update Package 10

The new feature addressed in JSA 7.5.0 Update Package 10 is listed below:

In JSA 7.5.0 Update Package 10, you can change the JSA user interface (GUI) theme to your preferred mode. To change the UI theme, go to the **Theme** drop-down in the **User Preferences** panel, and select the **Light** or **Dark** option.

Installing the JSA 7.5.0 Update Package 10 Software Update

JSA 7.5.0 Update Package 10 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 7.5.0.20241008193358.sfs file can upgrade the following JSA versions to JSA 7.5.0 Update Package 10:

- JSA 7.5.0 Update Package 8 SFS
- JSA 7.5.0 Update Package 8 Interim Fix 1
- JSA 7.5.0 Update Package 8 Interim Fix 3
- JSA 7.5.0 Update Package 9 SFS
- JSA 7.5.0 Update Package 9 Interim Fix 1
- JSA 7.5.0 Update Package 9 Interim Fix 2
- JSA 7.5.0 Update Package 9 Interim Fix 3

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 10 software update:

1. Download the 7.5.0.20241008193358.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 (10 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.
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 10 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 7.5.0.20241008193358.sfs.bz2
8. To mount the patch file to the **/media/updates** directory, type the following command:
mount -o loop -t squashfs /storetmp/7.5.0.20241008193358.sfs /media/updates
9. To run the patch installer, type the following command:
/media/updates/installer
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.

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 10 are listed below:

- WinCollect 7.3.1-43 upgrade fails.
- Access to X-Force servers.
- Upgrading to JSA 7.5.0 Update Package 8 or later from JSA version 7.2.x can fail due to insufficient disk space.
- Apps fail to restart after upgrade.
- Duplicate app entries on Traefik when JSA console is powered off and on again.
- Error messages appear during decapper startup in JSA Network Insights.

The following error messages on the terminal broadcast messages or decapper logs indicate an automatic fallback to a legacy decapper library on virtual hosts.

```
EAL: rte_mem_virt2phy(): cannot open /proc/self/pagemap: Permission denied
```

```
EAL: Cannot use IOVA as 'PA' since physical addresses are not available
```

This fallback is necessary when IOMMU and virtualization passthrough are not available and enabled in the virtual platform configuration. The decapper continues to function, possibly with lowered throughput.

- Autoupdates (AU) issue after upgrade to JSA 7.5.0 or later.

It is possible for autoupdates to revert to a previous version of autoupdates after you upgrade. Older versions of autoupdate might not update RPMs as expected. 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
```

For more information, see [Common Issues and Troubleshooting for Auto Update version 9.11](#).

- Issue adding Data Nodes to a cluster.
- Enabling the light theme fails to restore the previous color scheme.

Resolved Issues

The resolved issues addressed in the JSA 7.5.0 Update Package 10 are listed below:

- Performance degradation in 7.5.0 Update Package 9 Interim Fix 01 when you transition events between ecs-ec and ecs-ep components.
- After you upgrade from JSA 7.5.0 Update Package 7 to JSA 7.5.0 Update Package 9, the Pulse App does not have the proper permissions to run.
- Geographic rule test fails location match when IP is present in Network Hierarchy.
- Log rotate can fail in JSA 7.5.0 Update Package 8 due to a configuration conflict.
- Event Collectors with encryption enabled that drop connections to the Event Processor might experience event loss.

- User Account Deleted event doesn't contain information about the user who performed the action.
- The Notes in the Offense Summary CSV export are not in the correct order.
- Offline forwarding events fail with TCP over TLS when the event processor has no direct Internet access.
- Imported LDAP users are unable to receive emails due to the empty email field in users.conf.
- Blank page when adding an Ariel filter condition in a custom rule if the value ends with a backslash "\".
- In Log Activity right click filters won't display if the Source Address is IPv6.
- XML Expressions are unable to extract properties containing data after "&".
- After changing the server time on the command line of a JSA console, tomcat can get stuck on reading report templates and fail to fully start.
- JSA HA secondary hosts can go into a failed state after deploying changes.
- Missing some fields for CRE Rule Modified SIM audit event.
- JSA GUI can become unresponsive during a login attempt if the LDAP server is unresponsive.
- Custom AQL Queries are removed from Manage Search Results after a Full Deploy.
- Custom property deletion checker can incorrectly identify rule dependencies.
- Report summary displays the "Run this report when wizard is complete" option incorrectly on the report wizard.
- Deployments with multiple encrypted data nodes do not rebalance between each other as expected after an upgrade to JSA 7.5.0 Update Package 3.
- Changes made to the time series chat dashboard layout can fail to persist after logout.
- "AADSTS75011" error when you use Windows Hello by X509 without the auth context.
- JSA: Correlation Rules and Building blocks owned by disabled users do not execute in Update Package 9. No errors reported.
- Background deployment tasks triggered by LDAP user synchronization can block deploys initiated from the UI.

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 © 2025 Juniper Networks, Inc. All rights reserved.