

Release Notes

Published
2023-07-31

JSA 7.5.0 Update Package 2 SFS

Table of Contents

What's New in JSA 7.5.0 Update Package 2 | 1

Installing the JSA 7.5.0 Update Package 2 Software Update | 1

Installation Wrap-up | 3

Clearing the Cache | 4

Known Issues and Limitations | 5

Resolved Issues | 5

What's New in JSA 7.5.0 Update Package 2

For more information about what's new in JSA 7.5.0 Update Package 2, see [What's New Guide](#).

Installing the JSA 7.5.0 Update Package 2 Software Update

JSA 7.5.0 Update Package 2 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 7.5.0.20220527130137 SFS file can upgrade the following JSA versions to JSA 7.5.0 Update Package 2:

- JSA 7.3.2 (Fix Pack 3 - Fix Pack 7)
- JSA 7.3.3 (GA - Fix Pack 11)
- JSA 7.4.0 (GA - Fix Pack 4)
- JSA 7.4.1 (GA - Fix Pack 2)
- JSA 7.4.2 (GA - Fix Pack 3)
- JSA 7.4.3 (GA - Fix Pack 5)
- JSA 7.5.0 (GA - Update Package 1)

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 2 software update:

1. Download the 7.5.0.20220527130137 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 7.5.0.20220527130137.sfs.bz2
8. To mount the patch file to the **/media/updates** directory, type the following command:

```
mount -o loop -t squashfs /storetmp/7.5.0.20220527130137.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.

Result

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 2 are listed below:

- If your network connection is behind a firewall, the App Host is unable to communicate with your Console.

There is no workaround currently.

- After you install JSA 7.5.0, your applications might go down temporarily while they are being upgraded to the latest base image.
- Log Analytics is missing from the installation wizard menu.
- The console displays as an event collector in the System and Licensing, License Appliance Type column.
- Factory reset flatten, wipe, and retain menu options are missing, and flatten is performed automatically. Do not select Factory Reset from the Grub menu unless this is the intended action, as there is no workaround or recovery. Ensure configuration and/or data backups are enabled and regularly copied off the appliance.
- The software menu displays unsupported functionalities.
- The appliance menu displays unsupported functionalities.
- Under certain conditions, the installation will fail on JSA7500 and JSA3800 with the following error: "FileNotFoundException: [Errno 2] No such file or directory: '/proc/2108/cmdline' System setup failed." There is no workaround. Please contact <https://support.juniper.net/support/>.

Resolved Issues

The resolved issues addressed in the JSA 7.5.0 Update Package 2 are listed below:

- QRadar app install fails with 'No token header present in request...' error after 30 minutes.

- Asset list can fail to load when a null pointer exception occurs.
- Assets can fail to be updated with flow data as expected.
- LDAP group authentication can fail with special characters in usernames.
- LDAP auth can fail when LDAP group name has a special character and multiple groups assigned to same security profile and user role.
- Offenses no longer generated after restoring a deployment config backup and offense data from different dates.
- Log sources imported using the content management tool can fail due to password decryption issues.
- Python exceptions generated while attempting to add a data gateway.
- FIPS appliances with IMQ passwords containing '\$' can experience add host or deploy issues.
- Deleted managed hosts with an incorrect status in the JSA database can cause patches to complete successfully but with errors.
- The option to remove domain information from normalized event forwarding is not honored.
- Using the DSM editor to modify a configuration property for a specific event collector does not save the change.
- Repeated SSH debug messages can be observed in `/var/log/messages`.
- Online forwarding can leave behind stale TCP sockets if the connection is reset by the peer.
- Unable to retrieve maxmind geolite2-city.mmdb updates using a configured proxy in JSA.
- High availability appliance join can fail when the /store partition on the secondary appliance is busy.
- Offense 'save criteria' dialog box does not work due to specific interval value being 'null'.
- Events and offenses buttons are not highlighted on the device summary toolbar preventing searches.
- Deleting a rule in the Use Case Manager (UCM) app does not create an appropriate audit event.
- JSA vulnerability manager: Scheduled scans do not run after upgrading to JSA 7.5.0 Update Package 1.
- JSA vulnerability manager scans are not displayed on the scheduled scans screen.
- JSA vulnerability manager scan result export can include all scanned assets.
- Time series reports and dashboards not displaying data after the accumulator fails to load a globalview.

- Rules with network tests can sometimes fail to work as expected.
- Reference rule response stops working after all domains removed.
- Double match count flow rules can misfire due to IPv6 addresses being evaluated in rules before IPv4 addresses.
- Using a locale other than English, countries are not displayed in alphabetical order when modifying geographic rule conditions.
- Ariel searches in JSA can take longer than expected to complete when using a log source type filter.
- 'Runtime exception processing request get query status - querystatuswait' during ariel searches in JSA logging.
- JSA is affected by a remote code execution in spring framework.
- JSA can fail to pass events from ecs-ec-ingress collection process to the ecs-ec process.
- System notification for expensive custom properties fails to work as expected in JSA 7.4.2 and newer.
- Upgrades to 7.5.0 Update Package 1 can experience hostcontext issues due to unrestricted jce jar files.
- JSA patching to version 7.5.0 or newer can fail on managed hosts with "error: could not create unique index...".
- Issue reported when upgrading to JSA 7.5.0 Update Package 1 if the patch fails in patchmode.
- Upgrades on managed hosts can fail due to script connection timeout.
- Postgres re-install on managed host can fail after patching to JSA 7.5.0 Update Package 1.
- Patch installer fails with error message "Discovered extra databases which must be removed before continuing".
- JSA does not automatically clean up failed replication files in **/store/replication/failed**.
- JSA patch pretest fails to run on managed hosts until console is patched.
- JSA patching process can hang at message "updating : systemd-219-78.el7.x86_64".
- TCPV6 socket leak from real-time streaming causing tomcat outages.
- System rules might not display changes as expected from the UI or API.
- Cannot access remote networks and services configuration from the left tree menu.

- 'Application error' is displayed when accessing the admin tab when there is an empty file in **/opt/qradar/conf/licensekey**.
- After patching to JSA 7.5.0 Update Package 1, Vulnerability Assessment (VA) scanners no longer work.
- The software menu displays unsupported functionalities.