Release Notes

Published
2025-05-18

JSA 7.5.0 Update Package 9 SFS

JUNIPER NETWORKS | Engineering Simplicity

Table of Contents

What's New in JSA 7.5.0 Update Package 9

The new feature addressed in JSA 7.5.0 Update Package 9 is listed below:

In JSA 7.5.0 Update Package 9, the JSA user interface (UI) is updated to a dark theme. The light mode option is no longer available. This update does not affect the functionality of the product.

Installing the JSA 7.5.0 Update Package 9 Software Update

JSA 7.5.0 Update Package 9 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 7.5.0.20240719124908.sfs file can upgrade the following JSA versions to JSA 7.5.0 Update Package 9:

- JSA 7.5.0 Update Package 7 SFS
- JSA 7.5.0 Update Package 7 Interim Fix 1
- JSA 7.5.0 Update Package 7 Interim Fix 2
- JSA 7.5.0 Update Package 7 Interim Fix 3
- JSA 7.5.0 Update Package 7 Interim Fix 4
- JSA 7.5.0 Update Package 7 Interim Fix 5
- JSA 7.5.0 Update Package 7 Interim Fix 6
- 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 2
- JSA 7.5.0 Update Package 8 Interim Fix 3

NOTE: To successfully upgrade to JSA 7.5.0 Update Package 9, your deployment must be on JSA 7.5.0 Update Package 7 or later.

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 9 software update:

1. Download the 7.5.0.20240719124908.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 7.5.0.20240719124908.sfs.bz2

8. To mount the patch file to the /media/updates directory, type the following command:

   mount -o loop -t squashfs /storetmp/7.5.0.20240719124908.sfs /media/updates

9. A Leapp pretest, might be required based on your upgrade path:

   a. For JSA 7.5.0 Update Package 7 users updating to Update Package 9, type the following command:

   ```
   /media/updates/installer --leapp-only
   ```

   b. For JSA 7.5.0 Update Package 8 to Update Package 9 updates, skip this step. No leapp pretest is required.

10. To run the patch installer, type the following command:

    /media/updates/installer

11. 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 9 are listed below:

- WinCollect 7.3.1-43 upgrade fails.
- Pulse App upgrade fails on JSA 7.5.0 Update Package 9.
- NIC renaming when bonded during RHEL7 to RHEL8 migration.
- After upgrading from JSA 7.5.0 Update Package 7 to Update Package 9 with SSH, CLI session is down temporarily.
- High availability upgrades to JSA 7.5.0 Update Package 9 require a full DRBD re-sync after the upgrade completes.
- Upgrading to RHEL-8 on systems with LUKS encrypted partitions is not supported.
- Upgrading to JSA 7.5.0 Update Package 8 or later from JSA version 7.2.x can fail due to insufficient disk space.
- Leapp pretests do not verify sufficient disk space.
- Leapp pretests fail due to multiple physical network interface configurations.
- The e1000 network driver is not supported in Red Hat Enterprise Linux 8.
- Upgrade patch pretest fails on dual stack.
- Apps might go down during base image upgrade.
- Apps fail to restart after upgrade.
- Duplicate app entries on Traefik when JSA console is powered off and on again.
- Factory reinstall on JSA 7.5.0 Update Package 8 in the recovery partition fails.
- Managed WinCollect 7 agents cannot receive updates from encrypted JSA Managed Hosts with 7.5.0 Update Package 7 Interim Fix 05 and later.
- Error messages appear during decapper startup in JSA Network Insights.
- Autoupdates (AU) issue after upgrade to JSA 7.5.0 or later. For more information, see Common Issues and Troubleshooting for Auto Update version 9.11.

- Issue adding Data Nodes to a cluster.

Resolved Issues

The resolved issues addressed in the JSA 7.5.0 Update Package 9 are listed below:

- eps60s value is not set to 0 when the log source stops receiving events.
- CEP cannot be toggled for force parsing If a custom rule's name starts with a CEP name and it is used by another rule.
- Users cannot configure a test parameter for a rule when using a Reference Table.
- When deleting rules from API the username is truncated in audit log if the username include a period (.)
- The "Assigned to User" filter has been removed when editing "My Offense".
- An application error is observed when clicking a link in the "Top Category Types" dashboard widget.
- Assign offense menu showing as blank when trying to assign offense without log source access.
- Use case manager rules can be inconsistent with rules in the rule tab.
- AQL Custom Function Table Replication Issue in Data Gateway.
- False Positive flags do not reflect correctly in the rules.
- Customer with local language set as Simplified Chinese would run into offence page freeze.
- Modifying system rule leads CRE to throw NPE when reading dependant rules.
- Users who log in to JSA can receive an Error "Invalid license key" when the license is valid.
- Group Based LDAP Authentication does not preserve tenant assignment in User Details interface.
- Scheduled reports that contains more than three columns throws "Array index out of range" exception.
- Apps are in a failed state after upgrading to JSA 7.5.0 Update Package 7 Interim Fix 06 on a FIPS enabled system - not live.
- Failed to add HA on console when iscsi configured on Update Package 8 install - not live.
- Failed to add HA on a JSA 7.5.0 Update Package 8 console when an NFS mount is configured.

- HA synchronization status in 7.5.0 Update Package 8 is not displayed in System and License Management.
- Update Package 8 patch installer "--leapp-only" option does not support HA secondaries.
- Update Package 8 patch installer option "--leapp-only" will not run successfully on fresh Update Package 7 installations.
- Update Package 8 patch installer is unable to run "--leapp-only" option on a detached Console HA host.
- Events that bypass parsing will not have the correct collectorid.
- Cannot send udp syslog to QRADAR_CONSOLE_IP from app container on Apphost.
- UserDomainPermission_Test still impacts CRE performance after fix for DT212087.
- A boot loop can occur while patching to 7.5.0 Update Package 8 due to incorrect grub configuration.
- Cliniq failure on MH after RHEL8 migration causes patch to fail - not live.
- LDAP Authentication module can generate an 'Application Error' when saving changes in 7.5.0 Update Package 7.
- Natted deployments will fail to patch as Installer does not look at public IPs for checking if leapp-only was run.
- When patching to 7.5.0 Update Package 8, the RHEL8 Leapp migration script fails to remove the mptbase kernel module on VMware hosts.
- Expired user sessions preventing new logins.
- Change in QRADAR-17670 for CONFIGSERVICE_URL to fqdn causes replication to try public IP first - not live.
- Service scaserver is unable to start after migrating to RHEL 8 due to incorrect lib file.
- Patching to JSA 7.5.0 Update Package 8 can hang in environments using network address translation (NAT).
- JSA consoles running high availability with NFS mounts configured can fail "--leapp-only" tests when patching to 7.5.0 Update Package 8.
- Upgrades to JSA 7.5.0 Update Package 8 can fail if /storetmp does not have enough available disk space.
- Upgrades to Update Package 8 Interim Fix 01 might cause applications not to start due to podman-client-registry keystore corruption.

- 3148 AIO Console could have a CRE performance bottle neck.
- Custom actions scripts no longer work due to permission issues.
- Upgrading to JSA 7.5.0 Update Package 8 will fail on virtual hosts using an e1000 NIC adapter.
- A kernel defect is causing a significant search performance degradation issue in JSA 7.5.0 Update Package 8 Interim Fix 02.
- A deploy while HA is syncing will invalidate store and cause/restart a full sync - not live.
- When upgrading JSA to 7.5.0 Update Package 8, if an HA secondary host fails to reboot during the RHEL8 migration, the patch installer on the primary host will hang indefinitely.
- Missing langpacks in Update Package 8 cause API errors - not live.
- Services broken when Patched Update Package 8 host failover to Fresh Update Package 8 host due to UID changes in RHEL8 - not live.
- Log sources can sometimes display a status of error or not available when they are working as expected.
- Non-admin user cannot edit the group of log sources using the API when the security profile is set to all log source groups.
- JSA apps can randomly disappear from the JSA user interface.
- The "Not" operator used with the log source API does not properly filter results as expected.
- 7.5.0 Update Package 1 deployments with JSA Network Insight appliances can fail to deploy if the connection to JSA Network Insights is unavailable.
- Modifying the rule "Multiple login failures for single username" might cause a NPE error when JSA is reading the rule.
- `install-ssl-cert.sh` unable to install certificate signed by intermediate certificate authority.
- JSA filter "Source Network" displays an empty list in locales other than english.
- Destination IP/Source IP search parameter does not work with multiple IPs separated by comma in the Offenses tab.
- Apps can take longer than the default 90 seconds to start when 20 or more apps are installed.
- Timestamps on the Manage Vulnerabilities -> By Vulnerability Instances screen are incorrect - not live.
- Timestamps in a scan results (excel) report are displayed in the GMT timezone.

- Log sources status column might not update as expected, leading to stale or outdates status information.
- JSA Risk Manager: Unable to create a topology model.
- Offense tab columns do not sort as expected when search is set to default.
- Custom rules: Match count rules do not trigger as expectedly when used with coalescing log sources.
- Offenses created from flows rule does not show the first event in search result count.
- JSA non-administrator users cannot save changed to log source groups in the Log Source Management (LSM) app.
- Reports fail to generate when files other than images exist in /store/reporting/reports/logos.
- Admin tab can display an application error when assistant app cannot determine.
- Quick filter flow interface values can be duplicated for admins in the user interface when domains are configured.
- Data obfuscation can experience performance issues due to empty or null string checking.
- Bytes sent sorting for numeric custom property is filtered in the user interface as alphabetic.

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.