



RSA Governance & Lifecycle 8.0.0 P09

Release Notes

What's New

RSA Governance & Lifecycle version 8.0.0 P09 introduces features designed to enhance system efficiency, automate key tasks, and improve visibility. With updates like Duplicate Users and Accounts Notification, integration with RSA ID Plus (RSA Cloud Access Service), Stalled Requests Configuration, and Third-Party Library Updates, this release reduces manual intervention, optimizes performance, and bolsters security.

Highlighted Features

Duplicate Users and Accounts Notification

New event categories, **Detect Duplicate Users** and **Detect Duplicate Accounts**, have been added to Custom Events that notify/alert when the system detects duplicate users or accounts entries. While running a unification, and/or collecting data through ADC, the Custom Event Notification will be immediately triggered once a duplication (users, or accounts) is created. The selected or logged in user will be notified via Email and/or UI Notifications. This feature helps RSA G&L users to take fast action regarding duplicate entries as soon as they are discovered.

Integration with RSA ID Plus (RSA Cloud Access Service)

RSA Cloud Access Service (CAS) has been integrated with RSA Governance & Lifecycle. CAS is being introduced as an application inside RSA G&L. This integration connects the RSA G&L instance to CAS server and establishes a trust relationship between them, enabling subsequent bi-directional integrations.

For more information, see the [Quick Setup Guide - Connect Governance & Lifecycle to Cloud Access Service](#) on RSA Community.

Stalled Requests Configuration

Enhancements have been made to manage Stalled Change Requests under **Requests Configuration > Stalled Requests** tab. The existing Pending Change Requests custom event has been integrated into this tab to detect and notify when requests remain pending for extended periods. This tab provides two key capabilities:

- **Monitoring Pending Requests:** Integrates the existing Pending Change Requests Custom Event to detect and notify when requests are stuck for a long time.
- **Remediation (Cleanup):** Allows administrators to automatically move stalled requests to a **Cancelled** or **Completed** state based on configured thresholds.

These enhancements help to identify problematic requests before they impact operations, reduce backlog and improve system performance.

Enhancements

Feature	Description
ACM-134218	Logs have been improved around data source validation checks during WildFly based upgrades.
ACM-134076	Clicking Pause Scheduled Collections button from Collectors > Scheduling > Collectors page, now pauses scheduled Unification in addition to pausing scheduled collections.
ACM-133837	Data Purging process by default retains only five past versions of definitions of various types of objects, such as, collectors, agents, applications/directories, rules, business descriptions, etc. In P09, setting a custom flag keepVersionDataForMonths to a number will retain (and not purge) version data for the configured number of months.
ACM-132733	Application logs written in the database table T_AV_APPLICATION_LOG can now be capped to a maximum number of rows by setting a custom flag EnableMaxRowsThresholdForAppLogsTable to true (this flag defaults to false in all G&L deployments except for RSA G&L Cloud where it defaults to true) and configuring the maximum number of rows using another custom flag MaxRowsThresholdForAppLogsTable (defaults to 1000000). When this functionality is enabled and the number of rows in T_AV_APPLICATION_LOG reaches the configured max, any subsequent application logs are not written to the table until the number of rows reduce in the table, usually as a result of scheduled or manual Refresh Log. This feature affects only the log entries pushed to the table and does not affect writing logs to aveksaServer.log .
ACM-133225	A built-in mechanism has been introduced to validate the available disk space before applying patches, and an automatic clean-up for old patch files to free up space.
ACM-132598	Now, the Run IDs for the Duplicate User/Account removal task display the number of duplicates removed.
ACM-132591	Now, in the Cluster environment, Schedule Information lists information from all Nodes under Admin > Monitoring > Schedule Information .
ACM-132049	Improvements have been implemented to the Advanced Dashboards. <ul style="list-style-type: none"> • Drill-down filter options have been improved (more than one filter value and extended filter types). • Flexibility to set component headers has been implemented.

ACM-131970	If the user did not create/configure a Log Refresh Scheduler in the system, a default Log Refresh Scheduler has been created to run every day and purge the logs from T_AV_APPLICATION_LOG table that have existed for more than 7 days.
ACM-129665	In the Cluster environment, Thread Information lists information from all Nodes under Admin > Monitoring > Thread Information .
ACM-129664	In the Cluster environment, Database Statistics lists information from all Nodes under Admin > Monitoring > Statistics .
ACM-129662	In the Cluster environment, Memory Usage lists information from all Nodes under Admin > Monitoring > Memory Usage .
ACM-120380	In the Cluster environment, Performance Summary lists information from all Nodes under Admin > Monitoring > Performance Summary .

Fixed Issues

Issue	Description
SF-02710144 ACM-135173, ACM-133566	In the Active Directory Server , when a Group exists under CN=Users , the Add Account to Group Capability now works successfully.
SF-02699615 ACM-134363	Custom attributes now display properly grouped together by the separator defined under Admin > Attributes > Roles .
SF-02699967 ACM-134313	Deadlocks on T_AV_CHANGE_REQUESTS_MST object no longer occur due to database statistics operation.
SF-02695164 ACM-134155	In the RESTful Connector, when the parameter with multiple values used by the user which has double quotes ("dev", "admin"), it is now being relayed to the endpoint correctly and the additional slash characters are no longer being added to the data, for example ("dev\", "admin\").
ACM-134062	In the LDAP Connector, the connection timeout value has been changed from seconds to milli seconds.
SF-02693784 ACM-134041	In the RESTful Connector, the parameter used by the value provided for username parameter which has backward slash characters (username\\svc) is now being transformed to the endpoint as is . The backward slash characters are no longer removed.
ACM-133940	Importing SoD rules is working successfully if the review definition names match between the two environments (source and target systems).
ACM-133937	The logs of the Warning message "System property for Host name verification" have been converted to the Debug type, and the multiple logs of same message have been reduced.
SF-02695060 ACM-133924	In Java Code-Based Connector, the loading issue of MySQL and DB2 driver has been fixed for the endpoint connection. It no longer fails to load.
SF-02694718 ACM-133835	In the Generic Database Connector, the SQL query used by the user which has backward slash characters (domain\\username) is now being transformed to the endpoint as is . The backward slash characters are no longer removed.
SF-02680856 ACM-133833, SF-02672369 ACM-132362	Archival activity completes successfully, and the relevant history tables are created. Now, these history tables successfully display the archived data as well.
SF-02684231 ACM-133783	The Provisioning Node return status is now showing a comprehensible reason for Cancelling. It no longer gives the "Unexpected Exception" error.
ACM-133782	In the Generic REST Collector, empty or null values in the request header have been handled. It no longer gives the "java.lang.NullPointerException" error.

SF-02690670 ACM-133589	Responsibilities automatically assigned to the Business Owner and Technical Owner are no longer being missed.
SF-02691270 ACM-133580	The old Run ID of the Identity Data Collection (IDC) and Identity Data Unification (IDU) can now be opened successfully.
SF-02687943 ACM-133492	When the App Metadata Collector makes changes to Business Sources, it creates an entry in the applications_versions table. Now, the modified_by value is being set to system admin (AveksaAdmin) instead of any user in the system.
SF-02688775 ACM-133483	Encryption of passwords in domain.xml (WildFly) in Docker Container is now working successfully and the UI starts normally.
SF-02685548 ACM-133476	In the Active Directory Connector, support for multiple CNs in the DN has been added for Account and Group name-related activities.
ACM-132230, ACM-132201, ACM-128998	The following libraries have been updated: <ul style="list-style-type: none"> • The Log4j2 has been upgraded from 2.17.2 to 2.21.0. • The SLF4j has been upgraded from 1.6.6 to 2.0.17. • The jstl.jar has been replaced with jakarta.servlet.jsp.jstl-api-1.2.7.jar.
SF-02688968 ACM-133210	During the Account Data Collector (ADC) runs, the Indirect Relationships processing execution time is reduced.
SF-02685460 ACM-133123	Data Anonymization is now working successfully as expected. Errors no longer occur due to huge (90+) number of custom attributes.
SF-02684365 ACM-132996	The timeout of http binary downloader has been increased from 30 seconds to 2 minutes during the connector deployment process.
ACM-132865	In the Generic Rest Entitlement Collector with approle membership, the pagination is now being supported to handle multiple pages of entitlement data.
SF-02668887 ACM-132815	In the Generic Rest Entitlement Collector, the multi-level attribute mapping in resource and action is now being supported.
SF-02681986 ACM-132752	Calculate Role Metrics step in the Indirect Relationship processing run is now working successfully when there is multi-byte character present in the Role Membership.
ACM-132608	In the Salesforce Connector, Add Application Role capability is now being supported with both permission sets and profile names.
SF-02670615 ACM-132063	When grouping by Requested On and expanding the date, the UI now displays the correct Change Request which was requested on the relevant date.
ACM-130977	In the Generic REST Collector, the Page Number/Offset pagination method is now handling non- HTTP 200 response codes when the end of pages is reached.
ACM-124254	In the Generic REST Collector, only the important log messages are now being displayed in the log files. The restricted, repeated and irrelevant messages are being removed preventing enlarging the log files size.



Known Issues and Limitations

Issue	Description
ACM-135700	<p>After creating the first CAS application, the Refresh token does not work once the application is up after applying the latest P09 patch.</p> <p>Workaround:</p> <p>Restart the ACM application for the Refresh token to work.</p>



Platform Matrix

The latest application server and JDK version have been certified for this release.

	RSA Governance & Lifecycle Software Bundle	Software Only (WebLogic or WebSphere)	RSA Governance & Lifecycle Virtual Application	Container
Application Server Version				
WildFly 24.0.1 Included	Qualified	N/A	Qualified	Qualified
WebLogic 14.1.1.0	N/A	Qualified	N/A	N/A
WebSphere 9.0.5.21	N/A	Qualified	N/A	N/A
JDK Version Certified				
AdoptOpenJDK 1.8.0_472	Qualified	N/A	Qualified	N/A
Oracle JDK 1.8.0_471 (WebLogic)	N/A	Qualified	N/A	N/A
IBM JDK 1.8.0_471 (WebSphere)	N/A	Qualified	N/A	N/A
Operating Systems				
SUSE (SLES 12 SP5, and SLES 15 SP7)	Qualified	N/A	Qualified	N/A
Red Hat (RHEL 8.10 and RHEL 9.6)	Qualified	N/A	N/A	N/A

*RSA Governance & Lifecycle Virtual Application deployments are now supported on **Nutanix** through the **OVA file installation** method.



Prerequisites for Applying Patch (v8.0 P07 or Later)

Note: In case you are upgrading directly to P09 from patch P06 or earlier, you must perform the following procedure.

When using a customer-supplied Oracle Database, or RSA-Supplied Database installed remotely, update the AVUSER and AVCSUSER schema as follows:

1. Log in as SYS user (or another user with SYSDBA privilege) in SQLPLUS (or another database tool like SQL Developer).
2. Run the following script to grant permission on the following objects:

```
GRANT EXECUTE ON SYS.DBMS_CRYPTO TO AVUSER;
```

```
GRANT EXECUTE ON SYS.DBMS_LOCK TO AVCSUSER;
```

Note: If the AVUSER schema name is other than AVUSER, replace AVUSER with the appropriate schema name.



Product Support with Operating System

RSA Governance & Lifecycle version 8.0 P05 and later software bundle is now supported on RHEL 9.4+, however, RSA Governance & Lifecycle 8.0 must first be installed on RHEL 8, complete all the pre-requisites described below, and then upgrade the operating system from RHEL 8 to RHEL 9.4+.

Installing RSA Governance & Lifecycle on Red Hat 9.4+

Before upgrading your system from RHEL 8 to RHEL 9.4, ensure the following steps are completed:

1. Apply patch 8.0.0 P05 or later successfully on the existing RHEL 8 system.
2. Apply the latest Appliance Updater for Oracle Database to the existing RHEL 8 system containing the RSA-provided database.

After completing the upgrade to RHEL 9.4, ensure the following:

- The RSA-supplied JDK is installed and available.

The following packages are required for Red Hat Enterprise Linux 9.4 environments and may need to be explicitly installed in addition to the operating system.

binutils-2.35.2-43.el9.x86_64	make-4.3-8.el9.x86_64
gcc-11.4.1-3.el9.x86_64	sysstat-12.5.4-7.el9.x86_64
gcc-c++-11.4.1-3.el9.x86_64	javapackages-tools
glibc-2.34-100.el9.x86_64	lcms2
glibc-devel-2.34-100.el9.x86_64	rsync
ksh	syslinux
libaio-0.3.111-13.el9.x86_64	dejavu-sans-fonts
libaio-devel-0.3.111-13.el9.x86_64	dejavu-serif-fonts
libgcc-11.4.1-3.el9.x86_64	dejavu-sans-mono-fonts
libstdc++-11.4.1-3.el9.x86_64	fontconfig
libstdc++-devel-11.4.1-3.el9.x86_64	zip
libXi-1.7.10-8.el9.x86_64	unzip
libXtst-1.2.3-16.el9.x86_64	libns

Once all the pre-requisites have been completed as described above, start the RSA Governance & Lifecycle services.

RSA Governance & Lifecycle Product Version Lifecycle

RSA has a defined End of Primary Support policy associated with all major versions. For more details, please refer to the [Product Version Life Cycle for RSA Governance & Lifecycle](#).

As of RSA Governance & Lifecycle v8.0.0 P08, RSA G&L v7.5.2 is now EOPS.