Home (/S/)   Advisories (/S/Advisories)   Knowledge Base (/S/Knowledge-Base)   Documentation ⌄   Downloads ⌄   release notes P07 RSA Ready ⌄   Search Education (/S/Education-Servic   Login

ℹ **Learning Nuggets are now live!**   ✕

Explore quick, bite-sized, easy-to-follow, and free-of-charge learning materials that guide you through essential Cloud Access Service configurations.

Get Started (https://community.rsa.com/s/news/step-1-create-a-saba-account-MCOGWGWORRKVGDTM732D353LSW2E)

RSA Governance & Lifecycle 8.0 Patch 07 HF01 Release Notes

5 months ago

Note: RSA Governance & Lifecycle version 8.0.0 P07 HF01 is a replacement for version 8.0.0 P07 due to a potential failure in applying the P07 patch when public views in database schema include custom attributes (ACM-132849). The patch P07 is no longer available for download from RSA Community. The patch P07 HF01 can be applied directly to all previous patch levels, including P07, of RSA Governance & Lifecycle 8.0.0.

What's New

RSA Governance & Lifecycle version 8.0.0 P07 introduces features designed to enhance system efficiency, automate key tasks, and improve visibility. With updates like Anonymization of Terminated User Data, and **[Beta]** of User Access Review's new UX/UI, this release reduces manual intervention, optimizes performance, and bolsters security.

Highlighted Features

Anonymization of Terminated User Data

The data anonymization feature lets organizations anonymize details of identities (user records), stored in RSA Governance & Lifecycle, that have been marked terminated in RSA Governance & Lifecyle.

This feature removes all attributes of the selected terminated users and replaces with random hash values that are unrelated to the original data. Any data anonymized using this feature cannot be reversed to obtain the original data.

For more information about configuring and activating Data Anonymization, see the *Anonymization of Terminated User Data* Section in the Administrator's Guide (https://community.rsa.com/s/article/RSA-Governance-Lifecycle-Administrators-Guide-8-0).

New Reviewer UI for User Reviews – [Beta]

The feature is not intended for production use and is hidden by a custom feature flag named **FeatureFlag.UseEnhancedUIForReviews**. When this feature is enabled (only by Admin user), *from **Admin > System > Settings tab > Edit > Custom***, reviewers are provided with a toggle option, *from **Home > Reviews > My Reviews** page > **Use the new UI** toggle*, to allow experiencing new UI.

- When the toggle is turned **ON**, opening any user review will provide the new UI experience.
- By turning the toggle **OFF**, users will be able to perform the reviews using existing UI.

This feature will be extended to all other review types in later patches and will be the only option available when it is ready for production use.

This beta feature is available to all customers for testing. If you test the new UI, please send us your feedback or questions via **gl-beta-feedback@rsa.com (mailto:gl-beta-feedback@rsa.com)** *(mailto:gl-beta-feedback@rsa.com)*. *Please do not contact RSA Technical Support or do not open a Technical Support Case if you have any feedback on this beta feature.*

New Features

Feature	What's New
ACM-130357	If **AccountDNBase** and **GroupDNBase** are configured at the Domain Component (DC) level, without any specific Organizational Unit (OU), this is referred to as DC-level mapping. **Example:** • DC=RSA,DC=emc,DC=lab In such cases, account and group creation will occur directly under the specified DC path. However, for other operations (such as lock/unlock account, password reset, etc.), the system will first attempt to locate the account or group by performing an update-based search to determine the full DN (including its OU) and then proceed with the requested operation. **Example:** • **Input:** Account Name = "Test Account" • **Operation:** Lock Account **Behavior:** 1. The system will search for the full DN of the account named **Test Account** under the DC-level base. 2. Once found, it will then perform the lock operation on the identified DN. The functionality will support all the LDAP types.
ACM-130066	The functionality to add, update, and remove multi-valued attributes using the following parameters: • **add_<attribute>** • **replace_<attribute>** • **remove_<attribute>** In the endpoint, the request has now been extended to support all LDAP-type connectors, not just Active Directory (AD).
ACM-129576	The HXTT driver version has been upgraded from v7.1.234 to v7.1.255.

ACM-129501,
ACM-129500
	By default, the REST collector supports query parameter–based pagination, where pagination details such as, for example, offset, limit, and page are passed in the URL as query parameters.
	As part of this enhancement, **GraphQL-style** pagination is now supported, where pagination information is passed within the request body instead of the URL.
	UI Update:
	Pagination Mode Selection
	A new dropdown has been introduced to allow users to choose how pagination should be processed:
	• Query Parameter (default)
	• Request Body
	
	Default Behavior:
	The dropdown defaults to **Query Parameter**, maintaining the existing behavior.
	To Use GraphQL-style Pagination:
	1. Select **Request Body** from dropdown.
	2. Add the pagination logic within the request body's query field, for example:
	
	`{`
	`"query": "query { roles(limit: ${limit}, offset: ${offset}) { id name description } }"`
	`}`
	3. Configure pagination details as follows (*example*):
	
	    Max Records Per Page:
	    ◦ Parameter Key: *limit*
	    ◦ Parameter Value: *50*
	
	    Offset Details:
	    ◦ Parameter Key: *offset*
	    ◦ Initial Value: *0*
	    ◦ Incremental Factor: *50*
	
	    The request body will automatically generate the query with actual values internally, for example:
	    `{`
	    `"query": "query { roles(limit: 50, offset: 0) { id name description } }"`
	    `}`

ACM-129458	WorkPoint component has been updated to version 4.50.14.
ACM-127310	Users with Diagnostic entitlements (Diagnostics: Admin, Diagnostics: View) can run or view the Segment Advisor reports.

Feature	What's New
ACM-124750	RSA G&L now supports Data Anonymization. *You should log in to the Database as SYS user, and then execute the following command:* • `grant execute on sys.dbms_crypto to AVUSER;` • `grant execute on sys.dbms_lock to avcsuser;`

Enhancements

Feature	Description
ACM-130372	The **Database_Statistics.GATHER_DATABASE_STATISTICS** is now enabled to gather statistics for partition tables.
ACM-130321	A Validation has been introduced when setting the membership rule under **Roles > Global Roles > Members** tab.
ACM-130311	The user interface response time for the password reset process has been enhanced.
ACM-130249	UI has been improved in the **Purge** section, under the **Data Management** tab. The Schedule section has been removed, and the **Edit** button has been renamed to **Schedule**.
ACM-129831	When exported workflows included user data, references to those dependencies were not handled properly during the import of workflows to another environment, such as during a transition from on-prem to G&L Cloud. Now user data included in workflows can be properly handled during the export/import of workflows across environments (such as during a transition from on-prem to G&L Cloud) by setting a custom flag **HandleObjectReferencesInWorkflowsDuringExportAndImport** to **true** in the source and target G&L environments. This flag is set to **false** by default. The flag must be set to **true** PRIOR to exporting and importing workflows that include user data references.
ACM-129651	The Server Node page performance has been enhanced. The retrieval of log information for nodes in the cluster that are experiencing communication issues has been omitted.
ACM-129647	Data Archiving process performance tuning has been enhanced.
ACM-129367	The response time for User Requests has been enhanced.
ACM-129337	Performance improvements on loading of **Accounts** page.
ACM-124044	A new feature has been implemented that enables the default timezone for all users to be configured under **Admin > User Interface > Settings**. In the past, the default timezone was based on the system timezone of the installation site. Each user continues to have the ability to select their preferred timezone through the **Options > Date/Time**.
ACM-128406	The Clean Archive Source(s) are now displaying the **archive_id** under the **Monitoring** tab > **Data Runs**.
ACM-128279	The Watch Cleanup job, under **Admin > Workflow > Settings**, now closes open watches for change requests that are completely processed (for example, CRs in the states **Completed**, **Cancelled**, **Rejected**, or **Errored**). The clean up of such watches is in addition to the already existing notification functionality.
ACM-126936	Users with **DataManagement:Admin** entitlement is now able to either Activate or Deactivate the **Archiving** setting.

Fixed Issues "*in P07 HF01*"

Issue	Description
ACM-132849	The Database Schema Migration step while applying the patch, now completes successfully (no errors occur) when the Public Views contain Custom Attributes for User objects.
SF-02679743 ACM-132505, SF-02674252 ACM-132237	The scheduled Generic REST Collector that is configured with Token or OAuth is now working successfully (no SQL errors occur in the Aveksa Server Log).
SF-02674446 ACM-132170	The missing address attributes, such as *City*, *Zipcode*, and *Country*, for some users in Generic REST IDC collections, which also affected user accessibility, are now being correctly mapped, collected, and displayed to each user's data. Such certain attributes were missed during collection because the JSON response from the endpoint returned address data as a **LinkedHashMap**, whereas the code expected a **JSONArray**.
ACM-132064	The Token Refresh Schedulers no longer run in P07 HF01 for **Generic REST Collectors** marked **Inactive**.
SF-02660429 ACM-131488	The issue with the Generic REST Collector Configuration page slow loading has been fixed, as updating the Collector History table during each token renewal has been stopped.

Fixed Issues

Issue	Description
ACM-131681	For the **Create Account**, **Create Group**, **Update Account**, and **Update Group** operations, attributes containing a backslash (****) character are not supported over SSL connections when the **Skip Certificate Validation** setting is set to **false**, across all LDAP Connector types.
SF-02662037 ACM-131360	Account updates are now functioning correctly across all LDAP Connectors when the full Distinguished Name (DN) is provided, even in scenarios involving duplicate account names and DC-level **AccountDNSuffix** mappings.
SF-02658064 ACM-131321, SF-02645954 ACM-130452	In the Salesforce Collector, the SOAP request header of the URL to the endpoint, containing two entries of Authorization with an empty token value, causing endpoint connection failure has been handled.
SF-02658447 ACM-131252	Enhanced entitlement relationship mapping in the Generic REST Entitlement Collector (resource + action + account). Previously, only one resource-action pair was collected when multiple actions were mapped to a resource.
SF-02657792 ACM-131161	The email template body is now correctly populated for Approval Nodes that have **Request with reply** enabled buttons.
SF-02657740 ACM-131057, SF-02626035 ACM-129464	The AD **Account Creation** capability now supports all special characters (**$, &, #**) in the full Distinguished Name (DN).
ACM-130879, SF-02647937 ACM-130470, SF- 02622180 ACM-129192	The Restful Web Service connector is now working when using empty **${sessionID}** in capability configuration before the login API is called.
SF-02653398 ACM-130878, SF-02652095 ACM-130705	The Generic Database Connector configured with stored procedure is now working successfully when different parameters are configured starting with starting with same names.
SF-02632877 ACM-130868, SF-02642782 ACM-130242, SF-02608545 ACM-128753	The number of parallel processes and message consumption has been reduced to address the issue of CR items becoming stalled or stuck.
SF-02649668 ACM-130741, SF-02648968 ACM-130510	The Test Connection result for Active Directory Connector is now returned successfully without any maven jar dependency issue.
SF-02648612 ACM-130645, ACM-129984	The Generic Database Connector can be imported successfully when the group type is empty for the connector.

Issue	Description
SF-02648985 ACM-130637, SF-02644783 ACM-130310	On the Oracle Server Connector, the **add_**, **remove_**, and **replace_** attribute functionalities have been implemented for the **Update a Group** Capability.
SF-02649951 ACM-130599	The AD Connector settings using port 389 are now modifiable if the connector was created in an older version and then migrated to v8.0.
SF-02645833 ACM-130464	The Apache CXF component vulnerabilities have been fixed.
ACM-130426	The Access Key field for the JWT REST Connector is now displayed in an encrypted format, ensuring that the Key is no longer displayed in plain text on the connection details screen.
SF-02644775 ACM-130405	When the Command Output parameter is configured, the Database Connector is now working successfully (the account is created, and the configured query returns the data). Now, the Capability is working successfully when the **outparamater** is configured.
SF-02645450 ACM-130342	The unused vulnerable log4j version 1.2.13 has been deleted from maven cache in the AFX Server.
SF-02639578 ACM-130313	In the user selection dialog, users now can switch to simple mode if the **LIKE** operator has been defined on the department attribute in advanced mode. In simple mode, **LIKE** is represented as the Contains operator.
ACM-130303	Requests are no longer stuck in the AFX Fulfillment Handler Node when the output parameters are configured in Generic Database Connector.
SF-02602295 ACM-130272, SF-02623577 ACM-129390	In the AD Connector, when the LDAP Busy error occurred, the fulfilment request retry is happening only for requests with **Failure** state has been modified to include the **Failure** status code.
SF-02634247 ACM-130267	Under **Home > My Reviews**, raw HTML tags are now correctly rendered as formatted text in the Review view, instead of being displayed as raw code.
SF-02643106 ACM-130264	The AD Account update functionality now supports account names that include special characters (**&, $, #**).
SF-02641440 ACM-130245	The SQL Select Node now supports Common Table Expressions (CTEs) starting with 'WITH RS AS (...)' without errors when using public-level variables.
ACM-130244	Support for **AddAppRoleToAppRole** capability in REST Webservice Connector has been added.
ACM-130237	In the Workflow, when raising a Request via Webservice Call, the restriction in the Description field has been removed and the Request no longer fails.
SF-02641539 ACM-130223	The issue of the ASR generating duplicate entries, of the Collector information, has been fixed.
SF-02626440 ACM-130214	Terminated users can no longer access the report, even when the **Everyone** option is enabled during report configuration.
ACM-130157	Fixed the issue related to **Role Business Description** that occurred when two roles (one collected and one local) shared the same name leading to inconsistent info. With this fix, each role now maintains its own separate business description to avoid conflicts.
SF-02639384 ACM-130136	On the Role Summary screen, the **Action > Edit Attributes** wizard previously imposed a limitation on the text box length for attributes that exceeded 256 characters. This issue has now been resolved. The length of the text box will be according to the underlying attribute length.

Issue	Description
SF-02640400 ACM-130135	Proper error message is now displayed when the connector is configured to read a **JSONObject**, **JSONArray**, or **HashMap** from the REST response.
SF-02633110 ACM-130105	Importing Business Descriptions performance issue has been fixed.
SF-02636624 ACM-130103	When a Review Item is marked as **Maintain with expiration**, an exception/error no longer occurs and a task gets properly created to run on the Expiration Date provided, which will revert the Maintain with expiration and reopen the violation.
SF-02637728 ACM-130072	The **Update a Group** capability in the AD Connector successfully updates the Information attribute.
SF-02633091 ACM-130011	The **Discover Roles** function no longer ignores Technical Roles when using filters under suggested entitlement matching. The issue has been fixed.
Sf-02630237 ACM-129985	Support to pass the empty date value in the Generic Database Connector has been added.
ACM-129971	Regular users with System Admin privileges can now enable the Archive feature.
SF-02631497 ACM-129846	A Split job is visible on Change Request containing provision changes with grouping by Business Source.
SF-02631492 ACM-129845	In the AD Connector, the **Add Account to a Group** capability now accepts special characters (*****, **&**, **/**).
SF-02628648 ACM-129839	The Restful Webservice Connector can now handle the Json array with multiple values without any issues.
SF-02628030 ACM-129788	The **Application Name/ID** field, which captures data from multiple applications, has now been added to the Multi-App Generic REST Account Collector.
ACM-129773	In the Role Review Result, reviewers can now optionally add entitlements and generate the Change Request (Change Request generation no longer fails).
ACM-129768	The usage of upper case "SELECT" in "with" clause is now working successfully in SQL utility.
ACM-129690	Remote Agent and Remote AFX server now function properly when Proxy is configured.
SF-02629063 ACM-129615	AD Connection and all related capabilities, passwords containing special characters such as **< and >** are now supported across all functionalities.
SF-02626915 ACM-129455	Reviewer Details are now correctly displayed in the Email after the event completion.
SF-02621942 ACM-129452	The generation of incorrect Change Request Items to remove a Group from a User has been fixed in situations where the user is removed from a Role that includes Group Entitlement, and the user does not possess access to Group Entitlement.
SF-02610278 ACM-129377	The **Connection Closed** exception encountered while acquiring the LDAP connection has been addressed.
SF-02622180 ACM-129192	Fixed a null pointer exception issue when **${sessionID}** is configured without any prefix in the login API.

Issue	Description
SF-02623109 ACM-129186	Cancelling Out-of-Office for users is now working successfully; it no longer shows an error.
SF-02623258 ACM-129183	The Archive process now starts successfully due to changing the Comparison condition in the **From** and **To** dates used.
SF-02622931 ACM-129171	Performance tuning has been implemented to deploy the connectors faster.
SF-02601778 ACM-128201	The Generic Database Connectors are now successfully deployed when uploading custom **.jar** files.

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_452	Qualified	N/A	Qualified	N/A
Oracle JDK 1.8.0_451 (WebLogic)	N/A	Qualified	N/A	N/A
IBM JDK 1.8.0_451 (WebSphere)	N/A	Qualified	N/A	N/A
Operating Systems				
SUSE (SLES 12 SP5, and SLES 15 SP6)	Qualified	N/A	Qualified	N/A
Red Hat (RHEL 8.10 and RHEL 9.4)	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*)

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 and 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, assure 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	syslinux
ksh	dejavu-sans-fonts
libaio-0.3.111-13.el9.x86_64	dejavu-serif-fonts
libaio-devel-0.3.111-13.el9.x86_64	dejavu-sans-mono-fonts
libgcc-11.4.1-3.el9.x86_64	fontconfig
libstdc++-11.4.1-3.el9.x86_64	zip
libstdc++-devel-11.4.1-3.el9.x86_64	unzip
libXi-1.7.10-8.el9.x86_64	libns
libXtst-1.2.3-16.el9.x86_64	

Once all the prerequisites have been completed as described above, start RSA Governance & Lifecycle Services.

Follow

Related Articles

RSA Governance & Lifecycle 8.0 P07 HF01 Release Notes (/s/article/RSA-Governance-Lifecycle-8-0-P07-HF01-Release-Notes-pdf)

RSA Announces the Availability of RSA Governance & Lifecycle 8.0 Patch 07 HF01 (/s/article/RSA-Announces-the-Availability-of-RSA-Governance-Lifecycle-8-0-Patch-07-HF01)

RSA Governance & Lifecycle 8.0 Patch 06 Release Notes (/s/article/RSA-Governance-Lifecycle-8-0-Patch-06-Release-Notes)

RSA Announces the Availability of RSA Governance & Lifecycle 8.0 Patch 05 (/s/article/RSA-Announces-the-Availability-of-RSA-Governance-Lifecycle-8-0-Patch-05)

RSA Governance & Lifecycle Advanced Dashboards Library Release Notes (/s/article/RSA-Governance-Lifecycle-Advanced-Dashboards-Library-Release-Notes-pdf)

Trending Articles

RSA Release Notes for RSA Authentication Manager 8.8
(/s/article/RSA-Release-Notes-for-RSA-Authentication-Manager-8-8)

RSA SecurID software token .sdtid file fails to import into RSA SecurID Software Token 5.0 for Windows
(/s/article/RSA-SecurID-software-token-sdtid-file-fails-to-import-into-RSA-SecurID-Software-Token-5-0-for-Windows)

Unable to login to RSA Authentication Manager Security Console as super admin
(/s/article/Unable-to-login-to-RSA-Authentication-Manager-Security-Console-as-super-admin)

When replacing an RSA SecurID software token with a new software token the token PIN is not carried over to the new token
(/s/article/When-replacing-an-RSA-SecurID-software-token-with-a-new-software-token-the-token-PIN-is-not-carried-over-to-the-new-token)

RSA announces the availability of the RSA SecurID Hardware Appliance 230 based on the Dell PowerEdge R240 Server
(/s/article/RSA-announces-the-availability-of-the-RSA-SecurID-Hardware-Appliance-230-based-on-the-Dell-PowerEdge-R240-Server)

Don't see what you're looking for?

Ask A Question

RSA ID Plus (/s/topic/0TO4u0000017a3rGAA/rsa-id-plus)
RSA SecurID (/s/topic/0TO4u0000017a3sGAA/rsa-securid)
RSA Governance & Lifecycle (/s/topic/0TO4u0000017a3tGAA/rsa-governance-lifecycle)

Case Portal (/s/case/Case/Default)
Community Support (/s/community-getting-started)
Product Life Cycle (/s/product-life-cycle)
Support Information (/s/customer-support-information)

Contact Support
Terms & Conditions (https://www.rsa.com/terms-of-use/)
Privacy Statement (https://www.rsa.com/privacy/)