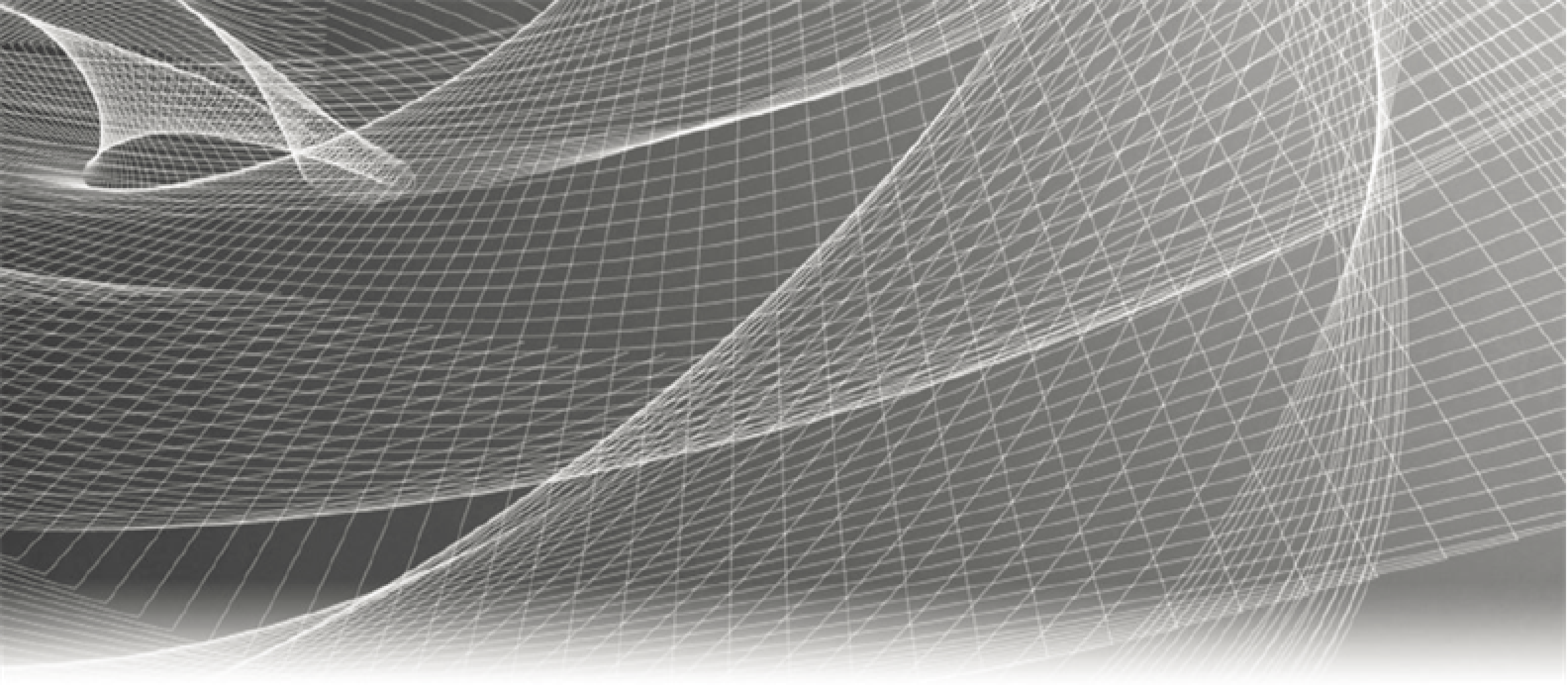

RSA IDENTITY GOVERNANCE AND LIFECYCLE

V7.1 Release Notes

Revision 1

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License agreement

Third-party licenses

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell Inc. believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

February 2018
Revised: June 2018

Contents

Revision History

Revision Number	Date	Revision
1	June 2018	Added note indicating that the version 7.1 installation files have been replaced with version 7.1 Patch 1.

Important Note About the RSA Identity Governance and Lifecycle 7.1 Installation Files

The base RSA Identity Governance and Lifecycle 7.1 installation files are no longer available, and have been replaced with RSA Identity Governance and Lifecycle 7.1 Patch 1. See the *RSA Identity Governance and Lifecycle 7.1 Patch 1 Release Notes* for the full details of the release.

RSA Identity Governance and Lifecycle 7.1 Patch 1 is available for download as both a patch and a full installation:

- To upgrade from a version earlier than 7.1, follow the instructions in the *RSA Identity Governance and Lifecycle Upgrade and Migration Guide*.
- For a new installation, follow the instructions in the *RSA Identity Governance and Lifecycle Installation Guide*.
- If you have already installed the base version of 7.1, follow the patch instructions in the *RSA Identity Governance and Lifecycle 7.1 Patch 1 Release Notes*.

Supported Environments and Components

The *RSA Identity Governance and Lifecycle Platform Datasheet and Support Matrix* for each version is available on RSA Link (https://community.rsa.com/). This document contains the most current details of the supported environments and components, including supported browsers and browser configurations.

Note: Internet Explorer 11 using Compatibility View is not supported. Internet Explorer 11 running Enterprise Mode cannot access RSA Identity Governance and Lifecycle.

Note: For optimal performance when viewing tables in RSA Identity Governance and Lifecycle versions 7.1 Patch 1 and later, RSA recommends using a supported version of Microsoft Edge, Mozilla Firefox, Google Chrome, or Apple Safari. If using a supported version of Microsoft Internet Explorer, limit the number of table rows displayed to a maximum of twenty.

Release 7.1

Information about the 7.1 release is included in the following sections:

- What's New in Release 7.1 below
- Deprecated Items in 7.1 on page 12
- User Interface Changes in Release 7.1 on page 12
- Fixed Issues in 7.1 on page 15

What's New in Release 7.1

The following sections describe the new features and improvements in version 7.1.

- Feature Highlights below
- Additional Features and Improvements on the facing page

Feature Highlights

Feature	What’s New
User Access Reviews	User Access Reviews have a new reviewer experience. The new reviewer experience provides a streamlined look that includes the Review Analysis and Guidance panel and advanced filtering. The Review Analysis and Guidance panel organizes review items into two sets of categories: Critical and General. Critical Categories identify review items that may pose a greater risk and that may require more attention during your review. General Categories group review items that may require less attention during a review. When creating a review definition, you can select either the new reviewer experience or the legacy reviewer interface.
Rule Mitigating Controls	If your organization has processes in place to reduce the risk of providing exceptional access to users, you can enable mitigating controls for separation of duties (SoD) and user access rules. When enabled, when maintaining exceptional access during rule violation remediation, remediators are required to provide details about the mitigating control used.
Workflow Dashboard	The page at Admin > Workflow > Monitoring displays information about workflows, and helps to detect problems by displaying warning icons if the workflow engine is unable to communicate with the database, if there are a large number of changes pending verification, or if changes have been pending verification for an excessive amount of time, if a workflow queue is potentially backed up, and if a workflow appears to be stalled.
Data Archiving	You can now create data archives to remove older data from active use within the RSA Identity Governance and Lifecycle system, while retaining a backup of the data to adhere to internal data retention policies or for auditing purposes. Archiving data reduces the size of the database and the

Feature	What's New
	resources needed by the database. Data archives can be used only for auditing purposes. Data archives cannot be restored to the RSA Identity Governance and Lifecycle system for troubleshooting purposes.
Password Vault	Support for using a third-party password vault to manage credentials for collectors, in addition to connectors, has been added. Support for several additional collectors and connectors has been added. To determine which collectors and connectors are supported by the password vault management, see the application guide or datasheet for the specific collector or connector.
Virtual Application	RSA Identity Governance and Lifecycle can now be deployed as a virtual application. The virtual application installation includes the application server and RSA Identity Governance and Lifecycle. Virtual application installations require a remote database.
Platform	The following platform updates have been made: • Support for SUSE Linux Enterprise Server (SLES) 12 SP2 has been added. New hardware appliances are built with SLES 12 SP2. Existing appliances running SLES 11 SP3 can upgrade to SLES 12 SP2 after upgrading to RSA Identity Governance and Lifecycle version 7.1. • Upgraded to Java 8. • WildFly has been updated to version 10. • Support has been added for WebLogic 12.2. • Support has been added for WebSphere 9.

Additional Features and Improvements

<table>
<tr><th>Feature</th><th>What's New</th></tr>
<tr><td>AveksaAdmin Password Security</td><td>After you upgrade or install RSA Identity Governance and Lifecycle, the AveksaAdmin password is hashed and encrypted in a new, more secure format upon the AveksaAdmin user's first login.
After a new installation or upgrade, you can migrate data containing the older password format only once. Attempting subsequent migrations may lock out the AveksaAdmin, and require assistance from Customer Support to recover access.</td></tr>
<tr><td>AFX-Install</td><td>File name validation has been added for connectors and connector templates. The following characters are not allowed in file names: \ / : * ? " < > |</td></tr>
<tr><td>Change Requests and Workflows</td><td>The following changes have been made to change requests and workflows:
• The workflow editor has been updated to Workpoint 4.4.0 Patch 10.
• A category attribute has been added for workflow definitions and jobs that support grouping. The category value can be set in the workflow editor.</td></tr>
</table>

Feature	**What’s New**
	- RSA Identity Governance and Lifecycle now manages workflows within several queues, which are automatically assigned based on the type of workflow. Workflows within a queue are processed in order. - The workflow editor now indicates the number of times a loop has been traversed. - The workflow editor by default displays only the active path of a workflow job. To view the entire workflow, deselect the Show Active Path Only option from the workflow editor menu. - SQL and Java node details are now only visible to users who can edit the workflow. - Rule escalation workflows now include the following nodes: Update work item, Activity, and Complete Assigned Work.
Collectors	The following changes have been made to collectors: - The Google Apps collector now supports the nickname attribute. If multiple values exist for nickname, the first value is used. - Users can now customize the Workday collector to configure attributes required for collection and map them to user attributes in RSA Identity Governance and Lifecycle.
Connectors	The following improvements have been made for connectors: - The audit log now includes events for creating, modifying, and deleting a connector. - Enhancements were made to improve how the REST connector handles headers and logins.
Custom Attributes	The maximum number of custom string attributes for group objects and business source objects have increased from 10 to 35.
Dashboard	After upgrading to RSA Identity Governance and Lifecycle v7.1, the new dashboard is displayed to users by default. If the previous deployment used the old dashboard, the old dashboard is disabled, but not deleted.
Database Management	The following changes have been made to database management: - Database statistics now exclude externally defined tables. - The public view PV_ACCOUNT now includes the collector name.
Data Collection Processing and Management	The following improvements have been made in data collection processing and management: - The way in which the identity collection and unification processes handle deleted users has been updated. Some relationships for deleted users remain mapped in the system for governance and auditing purposes.

Feature	What's New
	RSA Identity Governance and Lifecycle handles deleted users as follows: ◦ When deleted users are detected, the following relationships remain mapped in the system: • Account mappings that have been collected • Entitlements that have been collected • Local entitlements that are mapped to the user • Global role memberships that have been collected • Existing change requests that are in progress ◦ Any new relationship that is subsequently collected and mapped to the deleted user in the source system is accepted and mapped to the deleted user in RSA Identity Governance and Lifecycle. ◦ Deleted users are removed from all local role memberships. ◦ Imports of local entitlements that are mapped to a deleted user are rejected. ◦ Deleted users are not displayed in user selection dialogs. • When a data archiving job is suspended, an Admin Task alerts administrators that the data archive needs to be resumed. • The public view PV_ACCOUNT now includes the collector name.
Platform	Changes have been made to the aveksa_cluster script to improve the troubleshooting of clustering communication issues.
Reports	The Additional System Information section of the Aveksa Statistics Report (ASR) now includes a list of any custom files that have been uploaded.
Role Management	RSA Identity Governance and Lifecycle has made improvements to the export and import of roles. • Role imports and exports are now executed in the background, allowing the import and export of large numbers of roles without preventing users from performing other tasks while the import or

Feature	What’s New
	export runs. - When you export roles, you download a .zip file that contains one or more XML files containing role definitions. When you import roles, you can import either an XML file or a .zip file that contains one or more XML files containing role definitions.
User Interface	The following changes have been made to the user interface style: - You can display a header that contains a customizable logo, details of the logged in user and last login, and the Options, Notifications, Help, and Logout links by enabling the Classic Style user interface setting. - You can customize the look and feel of the user interface by uploading a custom CSS file. - You can add a custom background image to the login page by uploading a custom login-background.jpg file. - Custom files that are renamed are deleted are recorded under Audit Events.
Web Services	Web Service commands now support the JSON output format.

Deprecated Items in 7.1

Feature	Description
Platform	- Support for Red Hat Enterprise Linux version 5.*x* has been deprecated. Customers who have existing deployments on Red Hat Enterprise Linux 5.*x* must upgrade to a supported operating system. - Java 7 has been deprecated and will not be supported in future releases. RSA recommends that you upgrade to Java 8.

User Interface Changes in Release 7.1

The following table describes changes that affect the user interface or behavior of RSA Identity Governance and Lifecycle as the result of fixed issues.

Issue	Description
Access Certification	The Grouped by Application tab for a user review is now labeled "Grouped By Business Source." It now includes groups and roles organized by their directory or role set in addition to entitlements and application roles.
Access Certification	Bulk Actions now apply to accounts with unreviewed entitlements whether or not

Issue	Description
ACM-78225	they are signed off.
AFX	The SOAPAction header can be added through the UI or derived from the WSDL for each capability.
Authentication	Required challenge responses are validated and cannot be submitted if left empty.
Authentication	The external password reset tool will be case-insensitive when searching the following authentication sources: • RemoteADLogin • ActiveDirectoryAccountCollector • ActiveDirectoryIdentityCollector If more than one account name possibly matches the given identification for the sources above, the external password reset tool will then check for an exact match with case-sensitivity. If there is no exact match, an error message asks the user to type in the account name with the correct case. The password reset tool will be case-sensitive when searching other authentication sources.
Access Requests	The request cancellation date displays the Job start date.
Change Requests and Workflow	The Milestone Component now displays a change request approval step for canceled jobs.
Change Requests and Workflow	The workflow editor components change size when resizing the window.
Change Requests and Workflow	Group and role owner attributes can be added to subprocess node filtering.
Change Requests and Workflow	You cannot change or reset read-only jobs.
Change Requests and Workflow	Approvals and Activities, grouped by Business Source, and assigned to an application for "Directory for Account" use the application instead of the directory.
Change Requests and Workflow	The event type "Reject Changes handled by this workflow" is now available for Cancel Change Request nodes.
Change Requests and Workflow	An Edit button was added to the email body section of the email fulfillment handler configuration.
Collector	The Attribute category appears in the collector mapping page as intended.
Connector	AFX no longer enables a disabled user account after a successful password reset for LDAP connectors. However, AFX unlocks locked user accounts after a successful password reset.
Custom Attributes	The format of the metadata export file has changed to include additional custom attribute properties.
Data Collection Processing and Management	The Last Collected On field for individual accounts listed under an account collector now displays the last successful collection date, even if the data has not been updated since a prior collection. If an account has been deleted, the Last Collected On field displays the deletion date.

Issue	Description
Data Collection Processing and Management	The HasData option is no longer supported for new role data collectors. Existing collectors that currently use this option are not affected.
Descriptions	RSA Identity Governance and Lifecycle now requires that business descriptions for groups contain an application scope. When you create a new business description for a group that does not apply to a set, you must select an application with which to associate the business description before you can select the group. When you import business descriptions from an XML file, you must ensure that an application is specified for each business description that applies to a group. When updating or migrating RSA Identity Governance and Lifecycle from a previous version, RSA Identity Governance and Lifecycle deletes group business descriptions that are not actively in use. Before you migrate, run the provided pre-migration queries to identify any group business descriptions that will be deleted by the migration process. If you still need these group business descriptions, you can re-import them with an application reference in the import file, or you can manually recreate them after migration. For more information, see Migration Queries for Group Business Descriptions on page 38.
Metadata Import and Export	The User Attributes check box has been removed from the Import/Export dialog. All attributes, including user attributes, can be imported or exported by selecting the Attributes check box.
Reports	Report headers wrap column text to avoid hiding important information.
Request Forms	Support has been added for connecting to a web service using authentication when adding a field to an access request form. When you add a field to an access request form and select the control type "Drop Down select with Web Service", under Options, you can now configure the Authentication Type, Authentication User, and Authentication Password for the connection to the web service.
Request Forms	The Password Reset form can now process all field components that would create a change item.
Role Management	Users editing a role without access to the assigned roleset will see the assigned roleset but will not be able to change it.
Rules	• When remediating an SoD rule violation, you should not be able to alter your original action while the confirmation dialog is open. • Common entitlements are no longer detected in the entitlement coverage of a separation of duties (SoD) rule. As a result, SoD rules are not saved as an invalid rule. The rule detail page no longer displays a message containing the common entitlements between the two entitlement sets. SoD rules that are saved with the Invalid status are migrated to the Inactive status. When you import a rule that has an Invalid status, it is saved with an Inactive status.

Issue	Description
	On the rule configuration page, the following setting has been removed: "Allow execution of segregation of duties rules with common entitlements."

Fixed Issues in 7.1

The following issues were fixed in RSA Identity Governance and Lifecycle version 7.1.

Access Certification

Issue	Description
SF-803269 SF-927964 SF-979348 ACM-63517 ACM-75730	Specifying date-type attributes for user review criteria resulted in the following error: ORA-01840: input value not long enough for date format.
SF-835743 SF-915044 ACM-66520	The Grouped by Application tab for a user review did not display groups and roles by their directory or role set as expected.
SF-976100 ACM-76116	"Update Un-Reviewed Items" action in review item history showed AveksaAdmin instead of the actual user who performed the action.
SF-817109 ACM-64793	Reviewer delegation or reassignment comments greater than 4,000 characters in length prevented saving a review change with the JDBCException - ORA-01461 error.
SF-831090 ACM-67887	Reviewers with only "save" privileges and not sign-off privileges could not properly see review items queried by V_AVR_ER_ITEM_DETAIL.
SF-1008441 ACM-78070	The accounts and entitlements count displayed incorrect values when a reviewer applied more than one grouping.
SF-1037868 ACM-79267	The review results for user access reviews did not include the role entitlements for all users.
SF-1008019 ACM-78225	Bulk Actions did not apply to accounts with unreviewed entitlements if the accounts were signed off.

Access Requests

Issue	Description
SF-903529 SF-890332 SF-908531 SF-934592 ACM-71833 ACM-73254	In a form-based workflow where forms were approved and then fulfilled, the workflow intermittently skipped the approval step.
SF-942388 SF-955309	Revocation change requests did not display work items.

Issue	Description
ACM-73931	
SF-983142 ACM-75849	Rejecting one user in a request with multiple users during the approval phase removed too many pending accounts.
SF-917409 ACM-72808	Under Requests > Activities > By Entitlement and Requests > Approvals > By Entitlement, the Monitoring Policy view does not display activities for deleted accounts.
SF-823162 ACM-68232	The CSV file exported from Requests > Activities was corrupted.
SF-1025998 ACM-79262	Account removal triggered for a user with "Complete Manual Activity before collection" set to "Yes" did not completely remove accounts from user access before the collection.
SF-909706 ACM-72131	On the By Entitlement tab of the My Activities page, an account's custom attributes were not populated.
SF-959975 ACM-74600	The Fulfillment Handler was using the XML configuration instead of the internal configuration.
SF-898527 SF-1029461 ACM-73205	Manual workflow activity showed an incorrect timestamp when an escalation canceled the workflow.
SF-1063876 ACM-81061	A "Request could not be handled" error occurred when clicking on a submitted form request created via web service.
SF-865253 ACM-70239	The "last reviewed" or "completed on" date collected in a user access review was not displayed in the user access tab.

Account Management

Issue	Description
SF-894540 ACM-71583	After deleting account mappings, entitlements associated with the mapped accounts were still displayed under the User Access tab.
SF-894535 SF-941753 ACM-71731	Accounts that were mapped manually from an import file before upgrading could not be unmapped in bulk.
SF-910809 ACM-72136	The Oracle error ORA-06512 stopped the process when unmapping shared accounts.

AFX

Issue	Description
SF-1000278 ACM-77008	The AFX SOAP Connector used the wrong SOAPAction Header from the WSDL when multiple SOAPActions shared the same SOAP XML request body.
SF-1021681 ACM-79230	ServiceNow documentation needed additional details about permissions.

Authentication

Issue	Description
SF-854649 SF-851361 ACM-67933	Users that were deleted and then re-activated could not login using ADC authentication.
SF-982764 ACM-75796	A login with invalid credentials reported an error message with "account: {0}" instead of the account that could not log in.
SF-983896 ACM-75612	The query parameter SSOLogin=false, used to bypass SSO, no longer worked after upgrading to 7.0.2.
SF-1031227 ACM-78712	An error stopped the password reset if the Challenge Questions page did not validate mandatory questions that were skipped.
SF-1059055 SF-1059226 ACM-80559	Users had issues resetting a password because account names were not case-sensitive for an external password reset as they are for the login screen.

Change Requests and Workflows

Issue	Description
SF-943653 ACM-73734	In the new Workflow Editor, the context menu for workflow variables was missing the options Previous Node Assigned To and Previous Node Completed By.
SF-928182 ACM-73104	The number of escalations in a workflow was incorrectly limited.
SF-866742 ACM-69358	When creating a workflow for custom tasks, using the automatically populated Reference Name resulted in an error.
SF-842253 ACM-67139	Tooltip messages on a rejected change request incorrectly indicated that there was an error.
SF-950758 SF-958618 ACM-74131	When accounts were disabled, an incorrect change request item was created.
SF-874232 ACM-71674	When creating a change request, the user selection screen appeared twice when multiple forms were configured.
SF-889452 ACM-72560	The Cancel Change Request node for manual fulfillment workflows listed Reject Change Request selections that were not actually available for use.
SF-974919 ACM-75383	A sub-process node still expanded the workflow when the Enabled setting was unchecked.
SF-816607 SF-787423 SF-799534 SF-944220 ACM-67252 ACM-73747	A high workflow volume of excessive Oracle transactions could, due to a race condition, cause some workflow requests to be stuck in open state, stall on nodes like the Manual Fulfillment Node, or generate an ORA-02291 integrity constraint error.

Issue	Description
ACM-63718	
SF-956207 ACM-75139	In a manual activity workflow, a Mark Verified Node could erroneously complete verification of manual fulfillments.
SF-745588 ACM-60984	The user using the REST Web Services Node was unable to set "Content-Type", which instead defaults to "text/plain".
SF-920455 SF-910312 ACM-73174	When “Wait for Result” was selected, workflows were stuck in the Provisioning Command phase.
SF-895630 ACM-71205	Workflow Java node was unable to save configuration.
SF-845740 ACM-67829	After pending submission change requests were removed by a clean-up task, the pending accounts were deleted but the dependent change request items remained.
SF-913090 ACM-72140	A group entitlement was not included in a change request when added from a role review.
SF-956470 ACM-74461	The workflow job history did not filter out jobs that were being deleted by the purge process, causing an ORA-01722 invalid number error.
SF-936413 SF-993165 ACM-73792 ACM-76475	An error could occur when all line items were rejected in a change request if the system processed the workflow before it could process the line item changes.
ACM-76117	Large workflows usually with more than 23 nodes could not be saved.
SF-974932 ACM-75348	The drop-down list of processes in a child workflow could not show a list of more than 100 processes.
SF-820520 ACM-66029	Duplicate 'remove' change items appeared from a request to remove a role from a user that had duplicated entitlements.
SF-988230 ACM-76091	The REST Web Service node could not use user data to process a response variable.
SF-988600 ACM-76630	The workflow editor would not allow an invalid workflow condition to be displayed on a decision node.
SF-1000082 ACM-76911	Passing null or undefined workflow variables between nodes may have been stopped by a null pointer exception error.
SF-906471 ACM-72817	Importing a workflow with the overwrite option did not update the workflow name.
SF-997361 ACM-77724	Conversions of decision nodes did not succeed unless performed during a patch upgrade.
SF-1017258 ACM-77999	A subprocess node did not handle the ability to add group and role owner attributes.

Issue	Description
SF-1025290 ACM-78311	An unprivileged end user could edit the workflow to approve requests.
SF-990759 SF-994652 ACM-76958	Account data change verification for the Windows Server accounts collector would abort after running for more than 16 hours.
SF-951308 ACM-77144	Non-numeric values in the wp_proci table's lu_id field caused the workflow job table to not display properly.
SF-1021962 ACM-78218	The URL workflow variable didn’t resolve correctly when an escalation was raised on a request workflow.
SF-847108 SF-895584 ACM-61009	Performance optimizations for AFX queries in Oracle 12c.
SF-042252 ACM-79705	A business owner assigned to an application could approve and reject other, unassigned applications kept in the same directory for accounts grouped by business fields.
SF-931653 ACM-73399	In a workflow, a resource could not be modified when a dependent Group, User, or Role could not be found on an imported server.
SF-917117 ACM-72339	In the Workflow Editor, saving SQL nodes with the variable type Public could result in the Oracle error: "ORA-00972: Identifier is too long."
SF-921304 ACM-72337	When configuring a decision node to check whether a workflow variable exists, the Right Operand field is incorrectly required.
SF-991315 ACM-76476	Concurrent processing of a role management database update and change requests risked an indefinite open state for change requests.
SF-999080 ACM-77324	Workflow Editor SQL windows did not resize.
SF-946297 ACM-73893	A user could edit a workflow email node and save changes with the Refresh button without the required privileges for both actions.
SF-965923 ACM-74833	A collector node in the workflow editor did not validate for a selected account data collector.
SF-921304 SF-952404 ACM-72550	The save button did not enable for changing the "Evaluated to true" checkbox on a decision transition unless another change was made to the transition.
SF-1018384 ACM-78740	Exclusion rules for a node did not properly apply to employees designated as a delegate by an out-of-office supervisor.
ACM-72111	Workflow form compilation errors occurred due to conflicts with ports secured by SSL.
SF-1044220 ACM-80257	A change request did not successfully complete if a business owner's rejection re-mapped the account name derived from the account template to the account's unique ID.

Issue	Description
SF-992247 ACM-76647	A rejected change request approval step did not display when the workflow had completed.
SF-1046799 ACM-79688	Workflow decision nodes always evaluated manually entered variables as false.
SF-906005 SF-1008529 SF-996290 SF-944962 ACM-71857	An SQL error occurred when saving changes to an existing workflow process if it contained a delay node that was created in an earlier version of the product.
SF-914725 ACM-72045	A workflow copied from another workflow did not carry over the email body of the "Send Email" node.
SF-1062447 ACM-81011	Changes to due dates, priorities, and status could use cached data instead of the updated data.
SF-1070592 ACM-81877	Email approval templates incorrectly encoded the Email Approval Reply text.
SF-1031265 ACM-81002	The Workflow configuration to select 'Use Process configured on' was not available in the drop-down options after they paged.
SF-1096258 ACM-83234	The event type "Reject Changes handled by this workflow" was not available for Cancel Change Request nodes.
SF-1018709 ACM-79677	The email fulfillment handler did not contain an option to edit the email body or add workflow variables.
SF-1101627 ACM-83545	A Delete Account change request could be marked as complete but still show a status of "Pending Action".
SF-1098925 ACM-83236	Imported legacy workflows created before version 7.0.1 had a legacy value not handled by the new architect editor.

Collector

Issue	Description
SF-881641 ACM-70617	When a collected date did not match a supported date format, the entire collection fails, and the error ORA-01830 is displayed.
SF-903111 ACM-71836	Lotus Notes collections failed when attempting to use SSL communication.
SF-919973 ACM-72616	The Accounts data table for an ADC incorrectly displayed the Last Collected Date after a successful run.
SF-890141 ACM-70748	The example string for the Oracle Database collector URL had a typo that replaced a forward-slash with a colon.
SF-021848 ACM-48713	The App Metadata collector was case sensitive when referencing the owner ID fields.

Issue	Description
SF-556737 ACM-45979	The App Metadata collector did not update a business owner reference when the business owner information was deleted and then added back since the last collection.
SF-967914 ACM-75176	Identity collection removed an account from the Access tab when a user was marked as deleted.
SF-915352 ACM-72796	Testing the connection for the Airwatch collector resulted in a JSON error.
SF-792018 SF-843886 ACM-63785	The activity owner did not save when creating a local entitlement collector. An edit was required to add the activity owner.
SF-964094 ACM-76458	After installing RSA Identity Governance and Lifecycle, the identity collector would not connect to Novell IDM.
SF-991315 ACM-76565	For a change request that failed due to an invalid CR_ID, the review submission did not roll back updates to the database as expected.
SF-1003979 ACM-77722	The application metadata collector could not use the "category" attribute of an application for collections.
SF-999750 ACM-76886	Deactivating an existing data access collector from the General tab discarded settings for user and group resolution rules.
SF-00909993 SF-00907746 SF-00906213 SF-00915126 SF-00917341 SF-00929895 ACM-71772	ADCs are failing with the following error: “Unprocessed Continuation Reference”.
SF-795126 ACM-62974	Application metadata collections of wrong date formats for date attributes caused collection failures.
SF-1048233 ACM-80958	When using the Test button on a SQL query for a database collector, the screen incorrectly displayed a SQLException for a valid SQL statement.
SF-954031 ACM-78053	The transformer did not correctly create a CSV file for the CyberArk application.
SF-1039961 ACM-79634	The Salesforce collector did not collect LastLoginDate as expected due to an invalid date format error.
SF-1058274 ACM-80940	The WorkDay collector was failing with the following error: “Unmarshalling Error: unexpected element.”

Connector

Issue	Description
SF-882233	When a chain of certificates was involved in the handshake, the SOAP connector failed over 2-way SSL.

Issue	Description
ACM-71264	
SF-877139 ACM-70139	Attribute values edited to be blank did not carry over to the connector in attribute synchronization.
SF-966500 ACM-75158	Stored procedures called using a DB2 connector returned a null pointer exception.
SF-947029 ACM-74335	Unable to create a connector with a generic database using the DB2 connector template.
SF-973647 ACM-75745	AFX Connectors did not deploy when the connector dependency file ID exceeded 999.
SF-862539 ACM-70218	Disabled users were enabled after a password reset.
SF-973760 ACM-75597	The Archer connector did not deploy when the password to access had $ in the string.
SF-965812 ACM-75343	AFX requests for account creation fulfillment did not succeed due to "no signature of method" errors on the SOAP webservice connector caused by an encrypted password.
SF-1030498 ACM-79568	The SAP AFX Connector did not decrypt passwords when creating an account, preventing login with the password assigned.
SF-1045422 ACM-79915	The Lieberman EDC did not save the value for the Domain Name parameter.
SF-927034 ACM-73176	Users with multiple accounts in the same Active Directory database could not sync their passwords.
SF-807227 SF-1095978 ACM-64072	The Oracle AFX connector failed when a password contained the $ special character.

Custom Attributes

Issue	Description
SF-990118 ACM-76648	The PV_USERS view did not update with new custom user attributes.
SF-942744 ACM-73716	Some custom attribute properties, such as "In Detail," "In Popup," and "In Table" risked reverting to their default values because they did not copy to an exported file.
SF-850054 SF-1040785 ACM-70797	Custom attribute values for an application on the Summary page did not appear after uploading a customer strings file.

Dashboard

Issue	Description
SF-871409	The My Requests dashboard displayed incorrect values for All Requests, Pending, and

Issue	Description
SF-905933 SF-921603 SF-927362 SF-953819 ACM-70140	Completed.
SF-961911 ACM-74697	When the custom attribute ForcePageCleanup was used, "Request could not be handled" errors appeared when switching pages in the UI.

Data Collection Processing and Management

Issue	Description
SF-903491 ACM-71396	When a single expiration date for an account was collected in an unsupported format, the Active Directory collections failed.
SF-829704 ACM-66345	When an Active Directory account collection contained an attribute with a date value in an unsupported format, the entire collection failed.
SF-907379 ACM-71714	After enabling the Complete Manual Activity Before Collection feature, duplicate user entitlements appeared when the collector collected the added entitlements.
SF-854003 ACM-70365	When unifying multiple IDCs, some attributes are not populated.
SF-944541 ACM-73810	During collection, some groups could not be created when attribute values were null.
SF-907978 SF-919973 ACM-72044	After a collection failed, the Last Collection Date displayed the date of the last successful collection, but the Last Collection Status flag displayed the status of the most recent collection, regardless of its success. This could result in the Last Collection Date displaying the date of a successful collection, while displaying a red (failure) flag to indicate a more recent unsuccessful run.
SF-914637 SF-915168 SF-925035 SF-932268 ACM-71877	After upgrading, indirect processing failed due to duplicate entries of manually mapped accounts in the T_CE_EXPLICIT_RELATIONS table.
SF-874496 ACM-69828	Pagination was not working on the Attribute Synchronization page.
SF-968405 ACM-75062	When applying entitlements to a group and finding either sub-group members or groups that are entitlements in Collected Global Roles, group resolution was incorrectly case-sensitive.
SF-948261 SF-959587 SF-964145 SF-973841 SF-957979 ACM-73932	Identity collector could fail when USER_ID is used in a Unification Join.

Issue	Description
SF-955199 ACM-74460	Indirect Relationship processing did not reliably succeed because of Oracle error ORA-30926.
SF-954489 ACM-74783	A custom user-type attribute of a business source could get resolved to a terminated user if the custom attribute value did not distinguish the active or terminated user status.
SF-729636 ACM-57408	The MAEDC did not reject references to local applications.
SF-976294 ACM-75655	Indirect relationship processing of account changes for an ADC had performance issues and did not succeed when processing new account relationships.
SF-819318 ACM-65066	The collector did not allow edits because one of the collection data run tasks showed “in progress,” but no collection was actually happening.
SF-910243 ACM-71796	When a moved column value was too large for the new field, indirect relationship Processing for the Data Access Collector did not succeed due to error ORA-12899.
SF-993679 ACM-76572	A data type difference between two tables caused IDC Collector to not successfully collect due to ORA-01722: invalid number.
SF-985280 ACM-75977	A Change Verification job ran a long time for the Attribute Synchronization watches.
SF-964401 ACM-74754	The "Collect Identity" dialog box for selecting only non-mandatory collectors incorrectly implied that unification would run after collection.
SF-945246 ACM-74003	Collector configuration could not be modified, even when collection was not actively running.
SF-996452 SF-1008697 ACM-76856	Identity unification did not succeed because duplicate users caused unstable rows in the source tables.
SF-999529 ACM-77260	The group owner had to be processed again in later collections after a group collection did not resolve group owner values to a user.
SF-939467 ACM-73665	A collector may not finish processing due to error "java.lang.ArithmeticException: / by zero" when one of its internal processing files was between 8192 and 8195 bytes in size.
SF-991460 SF-998540 SF-752747 SF-981434 SF-902733 ACM-76508 ACM-60176 ACM-75770 ACM-77967	Collected IDC attributes were not being properly applied to the unified user.
SF-853028	The entitlement collector, when using a MySQL database as a source, did not correctly collect the approle memberships and entitlement relationships.

Issue	Description
ACM-68135	
SF-1025190 ACM-78293	The application metadata collector did not successfully run on a database with a large history of data runs.
SF-985551 ACM-76498	During IDC processing, new users were sometimes not properly processed into the table T_RAW_USER, and this caused missing unified user attributes.
SF-831492 ACM-66204	Collected user accounts mapped to unique identity attributes, such as email address, were not unmapped and orphaned when the value of the identity attributes changed.
SF-758832 ACM-62291	When the truncate data option is selected, strings with multi-byte data are not properly parsed.
ACM-78555	Benign errors stating "unable to find an attribute length" displayed in the logs when running collections.
SF-906377 ACM-77158	In some cases, users moved from lower priority IDC to higher priority IDC (and vice versa) created duplicate identities in the data.
SF-944339 ACM-73752	When importing a user account mapping for an orphan account, the new mapping was not reflected in the Total Orphan count in the application’s General tab.
SF-1044348 ACM-80237	Unification did not complete due to duplicate entries that caused unstable rows in the source tables.
SF-1027126 ACM-78580	The ADC occasionally performed poorly in runtime when validating data on step 2 of pre-processing.
SF-1073461 ACM-81946	User access table could not show entitlements of manually mapped accounts.
SF-628040 SF-680992 SF-654543 SF-690382 ACM-54093	Collection of AD date-time attribute values did not properly convert to the Aveksa server time zone.
SF-1018130 SF-1034638 ACM-79114 ACM-78727	User type attributes did not correctly display the User name, but showed the ID instead.
SF-1083500 ACM-82456	Excessive memory usage during RDC processing caused the Oracle error "ORA-04030: out of process memory”.
SF-1072789 ACM-81847	After an upgrade, an Oracle error for an oversized column occurred when running the ADC and calculating relationship changes.
SF-746902 ACM-58736	The long business description of an application did not show on the editing screen after it was collected.
SF-1055180 ACM-80332	Unification performance issues occurred in an IDC hierarchy with multiple joins.

Issue	Description
SF-1077479 SF-906377 ACM-83014 ACM-77158	Unification duplicated users with new records and terminated the original users when users moved from one IDC to another.
SF-1058100 ACM-80563	When a user was moved from one IDC to another, unification terminated the original user and created a duplicate user.

Data Governance

Issue	Description
SF-955928 ACM-74779	Users with both monitor and reviewer roles lost review items after reassignment from reviewer to monitor.

Database Management/Performance

Issue	Description
SF-889066 ACM-71028	During the merge users step of the unification process, performance was degraded.
SF-668203 SF-798389 ACM-53477	The fulfillment_phase_start_date and approval_phase_completed_date columns in the CHANGE_REQUEST public schema were not populated correctly until the request was completed.
SF-856272 SF-920947 ACM-68175	After clicking the Add Members button in a role, the Suggested Members view took over 20 minutes to load the list of users.
SF-902331 SF-965884 ACM-72071	Performance issues occurred when attempting to load entitlement records for a change request form.
SF-816551 ACM-68878	The Aveksa Statistics Report incorrectly reported the system hostname and IP when the remote database was updated with a database dump from another machine.
SF-968303 ACM-75048	Exporting the activity table could cause "Out of Memory" errors when there was a large amount of activity data.
SF-629019 ACM-72836	If columns for user data such as the first or last name were used, a user accounts table may not have displayed properly after an upgrade to 7.0.1 or later.
SF-924000 ACM-74184	File import data filtering enhancement.
SF-752469 SF-788597 SF-829125 SF-874464 SF-925700 SF-956468 SF-1004793 SF-1011605	Backup Jobs scheduled through the UI would stay in-progress and not complete.

Issue	Description
SF-1017008 SF-1030278 ACM-58925	
SF-795053 SF-883282 ACM-55401	The Aveksa Statistics Report did not report the correct sizes in the internal table summary.
SF-977818 ACM-75607	The V_DC_LATEST_FAILED_RUN view did not include collections that failed on circuit-breaker.
SF-1082570 SF-1091399 ACM-82474 ACM-82979	Exports through either the command line or the user interface failed if the process was previously interrupted and then started again.

Descriptions

Issue	Description
SF-864475 ACM-69179	Business descriptions for groups were deleted by the system during post-collection processing.
SF-881726 SF-948364 SF-912703 ACM-70178	Imported group business descriptions disappeared after collection.
SF-934145 ACM-75847	The overwrite option to import business descriptions for application roles did not work.

Email

Issue	Description
SF-865404 ACM-69677	Emails containing non-ASCII (UTF) character encoding were not sent properly.
SF-833463 ACM-66241	When a multi-step review was generated, the SecondStep Review triggered the NewReviewGeneratedEvent twice, resulting in duplicate e-mails.
SF-846422 SF-952095 ACM-68937	When the approver node in an access request workflow used Email Reply Processing, an HTML email response could not be parsed correctly.
SF-950680 SF-957202 SF-958008 ACM-74072	After a workflow update using the Workflow Editor, activity nodes in the workflow could not send email.
SF-834136 ACM-69395	Email nodes in a request workflow, which were not processed within an approval workflow, sent messages with blank role names.

Issue	Description
SF-955052 SF-945843 SF-969211 SF-983060 ACM-73143	Source edit attempts for workflow email HTML did not consistently work.
SF-820417 ACM-65032	When multiple reassignments were done at once to different users with different comments in a review, only one of the comments was included in emails sent to the users.
SF-922103 ACM-72618	When using the OptionalComments variable in an email template, approval comments were repeated within the email for each work item in the request.
SF-988027 SF-997491 SF-973366 SF-969211 ACM-76487 ACM-76609 ACM-76601 ACM-75170	International characters in HTML data prevented saves of email templates and email nodes.
SF-977178 ACM-75978	Excessive PasswordResetEvent and PasswordExpirationEvent ERRORs filled the aveksaServer.log file and delayed startup and shutdown.
SF-1004206 ACM-77308	Password resets issued by the administrator sometimes incorrectly displayed a 3-character password for the user accounts due to special characters in the view page.
SF-1010051 ACM-77547	When the email template AdminErrorNotificationMail is modified, that template could not populate the variable fields in the body when sending the admin Error email.
SF-932643 ACM-73930	Email events generating emails in a non-English could not change the language of the hyperlink text from English.
SF-1014915 SF-1014903 ACM-77735 ACM-77736	An encoded approval response was sent to a change request email approval.

Installer

Issue	Description
SF-832386 ACM-70244	Installer and uninstaller removed Aveksa_System.cfg, which rendered the staging folder unusable for reinstallation.
SF-888171 ACM-72528	ITIM Agent 7.0.1 did not start after installation due to a Java class error.
SF-995380 SF-1000210 ACM-76587	Could not complete the migration to version 7.0.2 Patch 1 when Oracle 12c database compatibility is set to a value lower than 12.1.

Issue	Description
SF-872354 SF-877589 SF-888160 ACM-69405	During a new installation, if the Oracle UID, oinstall GID, or both are not the default value of 500, the install script performs chown -R /tmp/Aveksa/staging to oracle:oinstall, regardless of the current ownership.
SF-1045387 ACM-79591	An XML parsing error occurred in UI settings data for a given user when applying a patch.
SF-1052918 SF-1063628 ACM-81060	The Oracle error ORA-01439 stopped initialization due to custom attributes with incorrect data types.
SF-1078101 SF-1053551 ACM-81325	The patch build number did not update after applying a patch, which caused patch processing to reoccur at startup.
SF-970037 ACM-76001	Duplicate files in aveksa.ear caused errors when deployed.
SF-942673 ACM-73935	The installation or upgrade process would get stuck when one or more required install packages were missing.

Localization

Issue	Description
SF-895722 ACM-71558	The Sample Date form displayed "NaN" in some fields when the browser language was set to a non-English language.

Metadata Import/Export

Issue	Description
SF-1011478 ACM-77437	Large amounts of workflow data in gigabytes risked a server time-out that disrupted a workflow import task.
SF-932143 SF-948063 ACM-73177	Importing incomplete export files of custom user attributes caused errors that affected creating new custom user attributes and running identity account collections.

Migration

Issue	Description
SF-950767 ACM-74441	The custom user attribute SUPERVISOR_NAME conflicted with an existing, identical attribute during a schema migration.
SF-976839 ACM-75848	During migration, the file ACM-60520.sql was running for several hours.
SF-974378 ACM-76009	An upgrade from 7.0.1 p2 to 7.0.1 p3 caused error “ORA-30926: unable to get a stable set of rows in the source tables” while executing the script database/migration/migrateReviewData.sql.
SF-974794	Database migration to 7.0+, when applying the ACM-61839.sql patch, did not succeed

Issue	Description
ACM-75390	due to Oracle error ORA-30926 because groups with duplicate names are no longer allowed when collected for the same application by different collectors.
SF-904759 ACM-71406	The migration screen did not clarify that the build versions shown refer to the database schema versions.
SF-897425 SF-995347 ACM-71062	A null pointer exception error could occur while viewing the migration webpage after clicking the “Follow Output” link.
SF-1098141 ACM-83172	Benign Oracle error ORA-06502 appeared when upgrading from an earlier release.

Password Management

Issue	Description
SF-873800 ACM-74080	In a RedHat environment with a remote database, users experienced slow user interface performance when updating challenge questions.
SF-929698 ACM-73096	Password policy was failing when the hyphen (-) character was included in the list of minimum required characters.
SF-942864 ACM-74782	Resetting a password using the Forget my Password link incorrectly sent daily reminders to the user, forcing the user to reset the new password again.
SF-1031229 ACM-79103	Password challenge questions allowed duplicate responses because they used to be case-sensitive.
SF-1067876 ACM-81469	A typo appeared in an error message.
SF-1039240 ACM-79546	A Windows Registry Notification Packages change for AD Password Capture tool caused a windows crash on a reboot.
SF-924320 ACM-73375	The View Password URL could not be correctly configured through the User Interface.

Reports

Issue	Description
SF-981041 ACM-75731	The scheduled report sent an empty report when using SQL parameters in the query and choosing CSV attachment types.
SF-942890 SF-976477 ACM-76875	ASR report generation from the UI did not succeed because the database hostname could not be resolved.
SF-922929 ACM-73707	The Reports tab was missing for users granted permission through the 'Run Report' and 'View Report Results' options on report definitions.
SF-792552 SF-883275 SF-847594	Filter criteria did not save when switching between the Query tab and the Filter Criteria tab.

Issue	Description
SF-916311 ACM-63502	
SF-978571 SF-992545 ACM-75807	A generated report did not use a new filter after it was applied.
SF-997123 SF-1041210 SF-1060770 SF-1060627 ACM-76633	The Aveksa Statistics Report generation stalled indefinitely after an XML parsing error.
SF-893547 ACM-71068	Text in the header row of a report was cropped and unreadable when a large number of columns were present.
SF-946294 ACM-73894	Sorting the reports table by the "Last Modified" column resulted in no reports being listed.
SF-973770 SF-1024500 ACM-75652	A custom scheduled report displayed results without applying requested modifications to the SQL query.
SF-1050335 ACM-80389	A user summary table took longer than expected to download from the UI.
SF-962852 ACM-74715	When trying to filter by group name in the Group Memberships report, the popup picker showed the list of report definitions instead of group names.
SF-868021 ACM-70441	The Global Roles Summary by Owner report erroneously included deleted roles.

Request Forms

Issue	Description
SF-918967 ACM-72683	Change request form could not be submitted if it contained required hidden tables.
SF-970650 SF-971399 ACM-75959 ACM-75226	The values of fields displayed but not enabled on a form did not show after the form was submitted.
SF-930848 ACM-73141	Could not access the Account Management form when the browser was configured to use a different default language than the RSA Identity Governance and Lifecycle server.
SF-984592 ACM-76631	Non-visual entitlement and account management tables incorrectly handled the shopping cart functionality.
SF-938295 ACM-73922	Action buttons on some entitlement screens had minor code performance issues when calculated.
SF-887157	Newly created Provisioning forms did not have user variables available in the list of

Issue	Description
ACM-70735	form fields.
SF-843527 ACM-67287	Fields could not be added to a request form using a web service with basic authentication.
SF-1010503 ACM-79564	A change request would not reflect a change in previously checked entitlements when using the back button to change the entitlements table filter provided from another component.
SF-1044516 SF-1047015 ACM-79555	When the user interface was displayed in Portuguese, the date selector did not work.
SF-1079363 ACM-82831	The Password Reset form only created change items for passwords and did not process field components that created other kinds of change items.

Role Management

Issue	Description
ACM-74064	When associating a role with a role set, the drop-down menu listed the raw names of the role sets, instead of the display names.
SF-897929 ACM-71048	The user interface displayed the Role Set Raw Name, instead of the expected Role Set Name.
SF-920150 ACM-72275	A change to a Role in a Role Set could not be reverted.
SF-965884 SF-964297 ACM-74834	Performance issues occurred when adding users and entitlements to a Role with active rules.
SF-928834 ACM-73183	The Add entitlements button became hidden in unnecessary contexts.
SF-941379 ACM-73630	When entitlements were added to roles through the Add Entitlements option in Actions, roles in role sets that restricted available entitlements could be displayed as selected, despite that the option was designed to pick only roles that allowed all Entitlements.
SF-968444 ACM-75121	Filters for entitlements and application roles did not function as intended on the second step of a multi-step user review.
SF-832188 ACM-66415	Role Discovery is not working in cases where entitlement matching criteria is not specified
SF-911427 SF-911459 ACM-73976	Users granted a role to edit entitlements could not remove entitlements.
SF-987410 ACM-76936	The role set table under Roles > Role Set showed the wrong values in the custom attribute columns.
SF-730647 SF-812390 ACM-57064	Role owner and group owner attributes were not available for selection when viewing all entitlements.

Issue	Description
SF-792647 SF-836164 ACM-65704	Role status remains in Applied or Applied New State, even after change request is complete.
SF-856943 ACM-68009	The exports of a large number of roles timed out before successfully completing the task.
SF-1007760 ACM-77310	A user without access to a role's assigned roleset could remove the unseen roleset when editing the role.
SF-987405 ACM-76935	The UI incorrectly displayed the raw role name instead of the role name on the Apply Changes and Commit Changes To Roles screens.
SF-1046008 ACM-80259	Local Entitlements could be deleted when associated with a role in the "New" state.
SF-1011117 SF-999469 SF-1001009 SF-1030252 ACM-77717	Entitlements could not be added to business roles due to an internal Oracle error.
SF-1067573 ACM-81344	Curly braces in the Column IDs table caused errors when sorting users by "Role Out of Constraint".

Rules

Issue	Description
SF-894858 ACM-71265	The Termination rule did not submit change requests to disable accounts for deleted users.
SF-916158 ACM-72138	Rule processing fails when a rule name contains a colon.
SF-928144 ACM-72795	Implicit Account Removal was not working as expected.
SF-945237 ACM-73882	The Confirm dialog box did not reflect any background data changes and allowed data submission that did not match the confirmation.
SF-966682 ACM-77504	Termination rule processing would not detect terminated users if multiple identity collections and unifications were scheduled sequentially through Web Services.
SF-881484 SF-934461 ACM-70087	Provisioning termination rule did not generate change requests for Disable Accounts and Revoke Entitlements.
SF-969733 SF-1015674 SF-858359 ACM-75786	A rule with an assigned remediator or a deleted email recipient caused a UI error when trying to view the rule details.
SF-1060767	The termination rule did not generate the expected change request to disable manually

Issue	Description
SF-1024622 ACM-80583 ACM-78296	mapped accounts.
SF-1045601 SF-1060217 ACM-79609 ACM-80718	The termination rule incorrectly generated change requests to disable accounts that were not assigned to a user.
SF-1017682 ACM-80224	The Attribute Change rule failed with an exception when generating a change request to add a local entitlement.
SF-1042701 ACM-79712	The Attribute Change rule did not generate a review when there is an existing review generated by the rule in an active or hold state.

Security

Issue	Description
SF-923995 ACM-72274	Multiple sanitization passes were required to fully remove disallowed HTML markup.
SF-924002 ACM-72278	The file upload function under Admin > User Interface did not restrict the types of files, potentially allowing unsafe files to be uploaded.
SF-924000 ACM-72276	Parameters containing URLs needed additional cross-site scripting filtering mechanisms applied.
SF-933060 ACM-73252 ACM-73250 ACM-73249	Users can bypass disabled buttons in the Diagnostics screen to view, download, and delete ASRs.
SF-866735 ACM-70721	After enabling secure session cookie configuration on a WildFly cluster setup, the Enable Secure Session Cookie setting displays No on the Security tab.
SF-1022650 ACM-78259	Applied properties to enhance security for an internal communications port used by a mule agent.
SF-1067853 ACM-81340	Fixed a security vulnerability specific to target users in the Out Of Office request forms.

User Interface

Issue	Description
SF-636368 ACM-52265	Color coding set as default by all users for rows defined by Control Type: Entitlement Table was lost if the user unchecked the Entitlement Type field in the table options.
SF-855386 SF-887226 ACM-67958	When using Internet Explorer 11 with Compatibility View or Enterprise Mode, the violation Revoke and Maintain buttons were disabled.
SF-1027542	Could not log in to version 6.9.1 using Compatibility View in Internet Explorer 11.

Issue	Description
SF-1022950 SF-1017658 SF-1028073 SF-1011890 SF-1023511 SF-1032885 SF-1023640 ACM-78552	
ACM-72791	Initialization status message contained a typo.
SF-858359 ACM-69870	A review definition could not be deleted if either the associated rule had a defined remediator or the email recipient was a deleted user.
SF-606336 ACM-51005	The error displayed when a Multi-App Account Collector was not configured to collect the business source reference did not clarify the collector at fault.
SF-932900 ACM-74704	A Lotus Notes resource in the Create Directory process described the directory component as an application in error.
SF-1065726 ACM-81745	The advanced search did not properly display the unequal sign if the browser or application language was not set to English.
SF-967960 ACM-76184 ACM-76185	Attributes did not display when searching in the Business Units or Application list.

Web Services

Issue	Description
SF-884876 ACM-70610	When the initial Register User web service was under load, it periodically failed to correctly pass variables into the workflow.
SF-953127 ACM-74334	SOAP requests sent to the ServiceNow Cloud through the SOAP web service node using proxy authentication were failing.
SF-981603 ACM-76590	A request to create an account from a Web service did not succeed when only one parameter was used.
SF-925848 ACM-72793	Benign errors appeared in logging for a service provider that was no longer in use.

Known Issues and Limitations

This section lists issues that remain unresolved as of this release. If a workaround is available, it is provided.

Tracking ID	Description
ACM-83961	While data collection works properly for DB2 and SQL collectors, test queries for these collectors result in errors.
ACM-73382	No warnings appear for empty or duplicate attribute names when importing a metadata file to a Wildfly environment. **Workaround**: Edit and save attribute names after importing a metadata file to successfully check that they are unique and not empty.
ACM-73246	[PUT] commands for very large file processes in a Wildfly environment do not execute because "request was larger than 128000." **Workaround**: Change the following attributes for application.yml: controllers: defaultScope: singleton upload: maxFileSize: 2000000 maxRequestSize: 2000000
ACM-54763	After editing an ITIM Connector, the Test Connector button reports a failed connection due to a "zip file closed" error. **Workaround**: Restart the AFX server and do not click Test Connection.
ACM-56715	The Archer Account Data Collector (ADC) does not collect more than one phone number when there are multiple phone number entries.
ACM-62715	In the Initialization Status window that opens when first starting RSA Identity Governance and Lifecycle after an installation or upgrade, the links to the log files do not work.
ACM-66476	When using the Compare User control, the target user is not displayed initially in the Change Summary table, in form details. **Workaround**: Navigate back to previous page, then select the detail page again, the user detail is displayed.
ACM-66521	When creating many collectors, a memory leak causes large amounts of memory to be used. **Workaround**: Restart AFX.
ACM-67400	The Admin menu disappears after importing metadata. **Workaround**: Log out of RSA Identity Governance and Lifecycle and then log in again.
ACM-62462	Applying Latest 7.0.0 P02 Build P02_7.0.0.106733, throws a java.sql.SQLException: "ORA-04068: existing state of packages has been discarded." **Workaround**: Restart the server and the application after you install the patch.
ACM-55664	Entitlements of the type global role cannot be added to a role in a role set, even though the Entitlement Rule setting for the role set allows that entitlement type to be added to

Tracking ID	Description
	the role.
ACM-52520	Only the Remove Change item is included in a request which was created to add and remove application roles for a user.
ACM-52471	When the Back button is selected in a request form, previously entered field values are not refreshed.
ACM-51564	The name of a reviewer selected in review definition disappears. It reappears in the review definition when the definition is subsequently saved and then re-opened for editing.
ACM-51562	Inconsistent bulk and single account review action results occur.
ACM-48298	When the "Allow Manual Activity to Complete before Collection" feature is enabled, the entitlement or application role is not added or removed.
ACM-62079	Total item count mismatch is observed under tabs for Approvals and Activities.
ACM-62306	The Entitlement Path under a user's Access tab shows an older account name and not the new, latest collected name.

Migration Queries for Group Business Descriptions

When updating or migrating RSA Identity Governance and Lifecycle from a previous version, RSA Identity Governance and Lifecycle deletes group business descriptions that are not actively in use. Before you migrate, run the following pre-migration queries to identify any group business descriptions that will be deleted by the migration process. If you still need these group business descriptions, you can re-import them with an application reference in the import file, or you can manually recreate them after migration.

Review the results of each query to determine if any of the identified business descriptions are still needed. You must manually recreate or import the identified business descriptions in the new system after migration is complete.

Unused Group Business Descriptions Not Associated with an Application

The following query identifies all group business descriptions that are not associated with an application, and that are currently unused. These business descriptions will be automatically deleted during migration.

```
SELECT
     id,
     'Group' as Type,
     object_filter AS "Object Filter",
     alt_name AS "Display Name",
     short_desc AS "Short Description",
     long_desc AS "Long Description",
     url_ref as "Help Link"
FROM
     t_av_business_description a
WHERE
     NOT EXISTS (
          SELECT
               application_id
          FROM
               t_groups b
          WHERE
               b.filter_id = a.id
          )
     AND a.scope_id IS NULL
AND a.is_deleted = 'FALSE'

AND a.object_type = 4

AND a.applies_to_set = 'FALSE';
```

All Unused Group Business Descriptions

The following query identifies all unused group business descriptions regardless of their association with an application. These business descriptions will be automatically deleted during migration.

```
SELECT

     id,

     'Group' as Type,

     object_filter AS "Object Filter",

     alt_name AS "Display Name",

     short_desc AS "Short Description",

     long_desc AS "Long Description",

     url_ref as "Help Link",

          (select name from t_groups where id =
          a.scope_id) as "Group Name",

          (select name from t_applications where id =
          a.scope_id) as "Application Name"

FROM

     t_av_business_description a

WHERE

     NOT EXISTS (

          SELECT

               application_id

          FROM

               t_groups b

          WHERE

               b.filter_id = a.id

          )

AND a.scope_id IS NOT NULL

AND a.is_deleted = 'FALSE'
AND a.object_type = 4

AND a.applies_to_set = 'FALSE';
```

Group Business Description Table

As the ACM schema owner, run the following SQL statement to create a table that allows RSA Identity Governance and Lifecycle to determine a group's business description state during migration.

```
declare

v_tbl_count number;

Begin

     select count(*) into v_tbl_count

     from user_tab_columns

     where table_name = 'TEMP_BUSDESC';

     if v_tbl_count > 0 then

     execute immediate 'drop table temp_busdesc purge';

     end if;

     execute immediate

     'CREATE TABLE temp_busdesc

          AS

               SELECT

                    name,

                    id,

                    filter_id,

                    application_id

               FROM

                     t_groups

               WHERE

                     filter_id !=-1';

end;

/
```