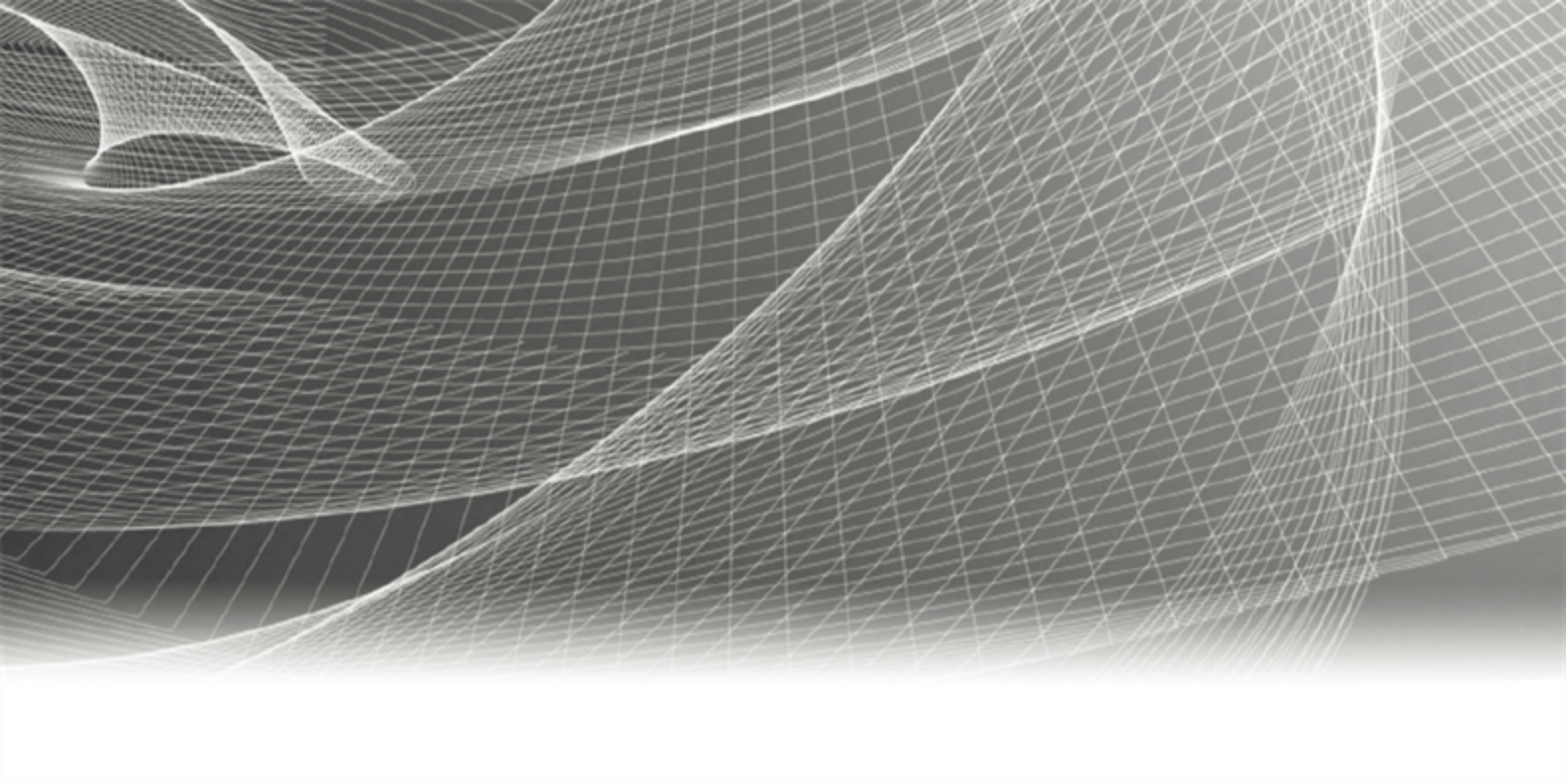

RSA IDENTITY GOVERNANCE AND LIFECYCLE

V7.1.1 Release Notes

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

Dell, RSA, the RSA Logo, EMC and other trademarks, are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License agreement

This software and the associated documentation are proprietary and confidential to Dell Inc. or its subsidiaries, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell Inc.

Third-party licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed by launching the RSA Identity Governance and Lifecycle product and selecting the About menu. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

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

Use, copying, and distribution of any Dell software described in this publication requires an applicable software license.

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 2019

Contents

Before You Install or Upgrade RSA Identity Governance and Lifecycle

Depending on your system and environment, you may need to perform some of the following actions when you install or upgrade RSA Identity Governance and Lifecycle.

- **Run the appliance updater.** Before performing an installation or upgrade of RSA Identity Governance and Lifecycle in an appliance deployment scenario, RSA recommends running the latest appliance updater. The appliance updater bundles a certified patch set for the operating system of an RSA appliance and the database on the appliance. Downloading and running these patches closes vulnerabilities and addresses bugs. The appliance updater does not patch the RSA Identity Governance and Lifecycle application. The patches are provided in a compressed file (rsaimg_updater_<*release_date*>_<*platform*>.tar.bz2) and posted on RSA Link at https://community.rsa.com/community/products/governance-and-lifecycle. Download and apply the appliance updater patches on a regular basis as new patches are released.

  For more information, see the *RSA Identity Governance and Lifecycle Appliance Updater Guide*.

- **Review certificate configuration if your deployment contains Active Directory collectors that use SSL.** The JRE has been upgraded to Java 8. By default, Java 8 enforces endpoint identification on LDAPS connections to improve the robustness of the connections. After upgrading, Active Directory collectors that use SSL that were previously able to connect might be unable to connect. View the aveksaServer.log for details about connection failures. If this occurs, ensure that the certificate of the host configured in the collector settings has the correct subject alternative name attributes available that match the hostname.

- **If upgrading RSA Identity Governance and Lifecycle in a WebLogic or WebSphere environment, you must update the AVDWDB data source.** Instructions are provided in the *RSA Identity Governance and Lifecycle Upgrade and Migration Guide*.

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.

Release 7.1.1

Information about the 7.1.1 release is included in the following sections:

What's New in Release 7.1.1

The following sections describe the new features and improvements in version 7.1.1.

Feature Highlights

Feature	What's New
Updated SOD Rules	Updated Segregation-of-Duty (SOD) rules and policy language, which includes additional analysis and detection capabilities to identify complex cross-application violations and reduce potential false positives. For information about the new SOD rules functionality, see "Using a Correlation Specification with a Segregation of Duties Rule" in the Online Help.
New Violation Remediation Experience	SOD and user access violations can now be remediated using violation remediation reviews, which allow users to review violations and perform remediation actions directly through the reviewer user interface. The violation remediation reviewer experience uses the same user interface as the new user access reviewer experience, which provides advanced features such as Analysis and Guidance, a review progress monitor, advanced filtering, and the ability to manage multiple violations at the same time. This feature uses both an SOD or User Access Rule definition and a User Access Violation Remediation Review definition and seamlessly manages their association within the system. For more information, see "About the Violation Remediation Review Experience" in the Online Help.
Display Views for User Access Reviews	Configurable display views are available in the new reviewer experience.
User Access Reviews	During user access review analysis, any review items with a pending revoke operation in progress are automatically marked with a revoke status.
Log Artifact Collection	Added automated log artifact collection and bundling capabilities to collect and send logs for support cases.

Feature	What's New
	This feature is available by going to **Admin** > **Diagnostics** and clicking the **Log Artifact** tab. For more information, see "Collect Logs to Review Artifacts" in the Online Help.
Diagnostics and System Data	System usage data, diagnostics, and heuristics information is collected and available through newly provided reports and through a downloadable JSON file for offline analysis and troubleshooting. You can configure this feature by going to **Admin** > **Diagnostics** and clicking the **Diagnostics and System Data** tab. For more information, see "Diagnostics and System Data" in the Online Help.
Web Services	The following changes have been made to Web Services: • A new series of web services are available for taking action on both approval and activity work items: performWorkItem, getWorkItemsForUser, and getWorkItemDetails. • The performApproval and performWorkItem web service commands allow any valid string as an action, which is validated against all supported transitions for the work item. • The getApprovalDetails and getWorkItemDetails web service commands now return the supported actions for the web service.

Additional Features and Improvements

Feature	What's New
Access Certification	The following changes have been made for Access Certification: • User reviews now leverage business calendars to determine when the completion due date is calculated and displayed. • The confirmation dialog for enabling or disabling an email template is now presented in a pop-up. • When a Maintain with Expiration action is performed on a review item, the expiration date details are now included in the Comments and History section.
Access Requests	A password reset for a user can be done by that user, an administrator, a user having the Reset Password entitlement, or the business owner or technical owner of the business source.
AFX	The AFX connector has improved performance when mapping unused variables in large environments.
Change Requests and Workflow	The following changes have been made in Change Requests and Workflow: • The number of work items retained in the workflow history is now limited to reduce the amount of data loaded. • The protocol for the URL specified in workpoint-client properties is now a variable and can be configured along with the URL and port.
Connectors	Introduced IBM Security Identity Manager 6.0 connector template for provisioning requests on ISIM.
Custom Attributes	The following changes have been made for custom attributes:

Feature	What's New
	• Custom attributes now have a reference name column, which stores an attribute name that unique across all attributes of the same type. The reference name cannot contain spaces, and any spaces detected are converted into underscores. In a new custom attribute, the reference name is automatically populated with the Attribute Name in which the spaces are replaced by underscores. This value is available for mapping in both Account Templates and AFX Connector Capabilities. This value is stored in the T_AV_CUSTOM_ATTRIBUTES table. • When upgrading or patching from a previous version, the Attribute Name values for a custom attribute are migrated. The Reference Name column is populated with the values of the Attribute Name with spaces replaced by underscores. • The Reference Name can only be modified during the creation of a new custom attribute.
Database Management	New custom attributes for strings and user data are available for resource objects: • CAS11 and CAS12 (varchar2), limit 4000 • CAS13 to CAS25 (varchar2), limit 256 • cau1 to cau5 (int) • cau1_name to cau5_name (varchar2), limit 512 For more information, see "Creating and Managing Attributes for RSA Identity Governance and Lifecycle" in the *Administrator's Guide* and the online Help.
Request Forms	The following changes have been made for request forms: • The Entitlement Table, Entitlement Table with Action, and Entitlement Table (non-visual) request form controls can now filter entitlements by entitlement types: entitlements, groups, roles, and application roles. This allows a finer scope and improved performance for the request form controls when only specific entitlement types are needed. • The way in which request forms for applications prompt for account information from end users has been improved. Users with only one account are not prompted to select an account. Users with multiple accounts are prompted to select an account as the first step, before the rest of the form is displayed. All aspects of the displayed application request form take the selected account into consideration, eliminating the need to select an account after selecting entitlements.
Server Core	aveksaServerInfo.log now includes the node name and environment name of the system, to assist with identifying the system from which the log originates.

Feature	What's New
User Interface	• New introductory text on the user interface clarifies how custom security contexts are implemented by RSA Identity Governance and Lifecycle. • Prominent warnings are now displayed if the reserved Custom Tasks capability is enabled.

Deprecated Items in 7.1.1

Feature	Description
Password Management	32-bit installation of the AD Password Capture tool has been deprecated.
Server Core	As of RSA Identity Governance and Lifecycle V7.1.1, OpenJDK 1.7 is no longer supported.
User Interface	Hardware appliance operations, such as edit, restart, reboot, and shutdown, can no longer be performed through the RSA Identity Governance and Lifecycle user interface. To perform these operations, use OS access level commands.
User Interface	RSA Identity Governance and Lifecycle no longer supports Internet Explorer version 10, due to the use of new technologies that rely on modern browsers. For a complete list of supported browsers, see the *RSA Identity Governance and Lifecycle Platform Datasheet and Support Matrix*.

User Interface Changes in Release 7.1.1

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 ACM-88680	The "Save Tab in Table" option has been removed from table pop-ups.
Access Certification ACM-87169	The new reviewer interface no longer includes access for terminated users as a low-risk category.
Access Certification ACM-88254	The user interface displays an "in-progress" indicator when general category bulk maintain actions are in progress.
Access Requests ACM-79721	Revocation change requests generated by account change requests will maintain the account property type.
Access Certification ACM-88929	Export operations are now limited to 5,000 records at a time.
Admin Errors ACM-92855	The Admin Error type "Account Load Data" can now contextually appear in the properties of a Create Admin Error workflow node.
Change Requests and	The default AFX Manual Fulfillment subprocess workflow now includes a job state node

Issue	Description
Workflows ACM-71049	to cancel change items when cancelling fulfillment.
Change Requests and Workflows ACM-80901	The number of work items retained in the workflow history is now limited to reduce the amount of data loaded.
Change Requests and Workflows ACM-88211	Workflows cannot be selected across different types of modules and are only selectable for the appropriate module type.
Change Requests and Workflows ACM-88351	The Show Job Level Variables setting in request workflows will not overwrite the same setting in approval and fulfillment workflows.
Change Requests and Workflows ACM-88384	A workflow must be removed from configuration (phase nodes, subprocesses, and escalations) before it can be deleted.
Change Requests and Workflows ACM-89649	The Business justification character limit has increased to 4000 while editing exceptional access.
Change Requests and Workflows ACM-89833	The fulfillment workflow now uses the correct query to group fulfillments by business source.
Change Requests and Workflows ACM-89860	WorkItemURL selection is now available for manual nodes.
Change Requests and Workflows ACM-90476	A custom task must be removed from the schedule before it can be deleted.
Change Requests and Workflows ACM-93462	The "Assign to" list no longer appears as available options for Resource Selection.
Collector ACM-75432	The attribute "lastlogontimestamp", always collected as a date-type value, can be stored in a custom attribute of either string-type integer value or a date-type value. A string-type integer value is automatically converted to the date-type value formatted as “yyyy-MM-dd HH:mm:ss”.
Data Collection Processing and Management ACM-74626	The Application Metadata Collector will only update application business source objects.
Data Collection Processing and Management	If an agent cannot resolve the Member Type from the Account Data Collector’s source system for a group’s member, it assigns "unknown" to the Member Type column in the raw data instead of guessing the correct member type.

Issue	Description
ACM-81403	When Member Type is "unknown", the collector's database processing still attempts to resolve the member type. If successful, it assigns a member type in the new "Resolved Member Type" column in the raw data. If Member Type is "unknown" and the member type cannot be resolved by the account collector, then Resolved Member Type is left blank and the collected membership is rejected.
Data Collection Processing and Management ACM-90663	The date range of historical configuration information has been reduced in areas such as collector changes.
Data Collection Processing and Management ACM-91761	The Last Reviewed Date OOTB attribute has been removed from the collector wizards.
Installer ACM-87123	Applying a patch overwrites the configuration files for plugins except for the ITIM2FulfillmentHandler, NovellIMListener, and SunFulfillmentHandler plugins, which are copied from the customer's system instead. The patch application process backs up the original plug-in configuration files in the folder **<location of the patch>/backup/<timestamp>/plug-ins/** so that you can restore them if needed.
Provisioning ACM-88777	The Workflow ValidReplyAnswers macro now populates and lists URLs in a consistent order.
Request Forms ACM-64863	The Request Forms wizard disables the Next button until all form elements on a page are loaded.
Request Forms ACM-70736	User filters containing avform.user variables are not replaced with substitute values in the Compare Users field of the Provisioning form.
Request Forms ACM-77882	Drop-down, Multi-select, and Number fields can be populated by avform attribute selectors used as the default value.
Request Forms ACM-83637	The JavaScript block form control no longer allows Display conditions. The Display tab for this form control displays a message for the restriction. When Enable conditions are set, the JavaScript block entered is executed only when the conditions are satisfied. If there are no conditions set, then the JavaScript block is executed whenever the form runs.
Request Forms ACM-88604	Multiple account resolution can be configured on a request form to prompt for every change or per business source.
Role Management ACM-75430	The Role Import process warns that collected roles, if imported, will be converted into local roles.
Role Management ACM-87106	The Out of Constraint Users list in the Analytics tab has changed to use the same format as the Users list in the Users tab.
Role Management	The "Role Missing Entitlement Rule" email notification now adds group entitlements

Issue	Description
ACM-74637	collected from the ADC.
Rules ACM-90043	An "Associate Remediation Job" button has been added to the Rule Details page for remediation actions. When clicked, remediation workflow jobs are created for identified and unassociated violations. This button is not enabled by default, but can be enabled by the "ViolationRemediationReProcess" feature flag.
Rules ACM-95300	Rules are now processed one at a time to avoid a system error. The monitoring page relays this new process as follows: Currently Processing Rule (X out of Y) Steps 1-3
Security ACM-73739	Enhanced security for page access in RSA Identity Governance and Lifecycle.
Server Core ACM-92902	The JRE has been upgraded to Java 8. By default, Java 8 enforces endpoint identification on LDAPS connections to improve the robustness of the connections. After upgrading, Active Directory collectors that use SSL that were previously able to connect might be unable to connect. View the aveksaServer.log for details about connection failures. If this occurs, ensure that the certificate of the host configured in the collector settings has the correct subject alternative name attributes available that match the hostname.
User Interface ACM-81449	The Other type for owners is now usable in simple and advanced views.
Web Services ACM-92041	Validation for webservice calls to add or remove accounts from a group can be requested using the collector or the business source, but not both.

Fixed Issues in 7.1.1

The following issues were fixed in RSA Identity Governance and Lifecycle version 7.1.1.

Access Certification

Issue	Description
SF-1044154 SF-1027351 ACM-82969	Change Requests in Open status without a workflow ID defaulted to the Explicit Access workflow after restarting the application.
SF-839034 ACM-66789	A review opened through an email link, then canceled, opened a null page after confirmation instead of the home page.
SF-855955 ACM-68187	Comments for review items could not be applied as part of a bulk update.
SF-1058478 ACM-82186	Triggering the Escalation Workflow of Review Reassign sent two emails to the user.
SF-1120715 ACM-84607	The email link to view a role review opened to an error page.

Issue	Description
SF-1124917 ACM-84693	A null pointer exception occurred when a reviewer opened the review using the email link, performed an action, then saved.
SF-1008666 SF-1027715 ACM-79783	Non-existent access to a group appeared for users in a User Access Review.
SF-597513 ACM-51149	Multiple Account Review attributes did not properly translate to other languages.
SF-1153118 ACM-86633	Revoking a user during a fine-grained role review resulted in a long delay before the status bar was updated.
SF-1110632 ACM-84590	Application coverage statistics showed incorrect values by not including roles and groups.
SF-1083271 SF-1176983 ACM-83163	After uploading a coverage file to delegate a sign-off to another user, duplicate Entitlements appeared in a User Access Review.
SF-1144992 ACM-85868	An on-hold role review that was closed without changes incorrectly marked a role as "changed".
SF-924608 ACM-72958	Group review results for monitors incorrectly displayed the member count for all groups as zero.
SF-1184310 ACM-88254	After performing bulk maintain actions on general category items, the user interface did not indicate that any action was in process. This caused the user to attempt to perform the action multiple times, even though it was already in progress.
SF-1167341 ACM-87169	The new reviewer interface included access for terminated users in the low-risk category by default.
SF-1190649 ACM-88508	The global table options for filters, groups, and columns did not work for the Reassign and Share Review functions in the new User Access Review interface.
SF-1195963 ACM-88680	A reviewer without required privileges could download the full list of users and attributes from any User Picker pop-up.
SF-1202327 ACM-89970	Large-scale reviews used all available memory and crashed the server with OutOfMemory errors.
SF-1202327 ACM-88929	Out of Memory errors occurred during large reviews.
SF-1205481 ACM-89536	A privilege column added to the reviewer coverage file of an account review definition did not appear in a .csv file saved from the data.
SF-1157646 ACM-86823	Reviews erroneously generated sign off reminder emails when reviewers were not allowed to sign off for themselves.
SF-1176460 ACM-87929	A reassigned review configured to allow a delegated user to sign off did not enable a delegate to sign off as intended.
SF-1239517	Review Generation for large datasets slowed in performance after an upgrade.

Issue	Description
ACM-91180	
SF-1173057 ACM-88464	Account reviews that generated change requests explicitly by owner did not properly create revoke item change requests if application business owners and directory technical owners were granted monitor access.
ACM-88164	A fine-grained role review for bulk revokes of role memberships with large user counts performed slower than expected.
ACM-92706	A bulk revoke action during a fine-grained role review on a role's user member or entitlement that was already revoked caused an error.
SF-1071410 ACM-81974	After disabling bulk actions on review items, bulk actions were not disabled on all review tabs.
SF-829112 ACM-66227	Reviews were not generated for users with no last name.
SF-1172050 ACM-87433	The default introductory text on the review escalation configuration screen was unclear.
SF-839401 ACM-66836	In the legacy reviewer UI, the Review Item Comments and History window did not display special characters properly. This issue is resolved for the new review experience.
SF-1172039 ACM-87438	Some reviewer escalation workflows were not triggered and the review history did not update if the review became active by an escalation workflow.
SF-1178009 ACM-90758	A reviewer listed in the Escalations Tab could not be found by the search tool.

Access Requests

Issue	Description
SF-964684 ACM-76816	Access Requests with violations could be submitted by requestors when the filter was defined with more than one role attribute.
SF-1021090 ACM-78198	Approval nodes assigned access requests to out-of-office supervisors if those supervisors were part of the approval workflow at another level.
SF-1102047 ACM-83563	Custom attribute value lists degraded the performance of rendering the User Access pages.
SF-01110863 ACM-84248	Attributes with "on" and no date caused an exception error during the display of the milestone on the Change Request Detail page.
SF-1066622 ACM-83225	An error occurred identifying the application name in a change request when the application had a Directory For Accounts setting.
SF-1122693 ACM-84601	A pending change request with a large number of new accounts could cause a cleanup issue when restarting.
SF-1098397 ACM-83297	A Review query was not optimized for large datasets and used too much database memory.
SF-818651 ACM-64918	Business Sources excluded from Add Access and Suggestions were visible under Requests > Create Requests > Add Access, but their entitlements could not be

Issue	Description
	requested.
SF-1042229 SF-1122224 ACM-80274	The manual activity assignment link became disabled after a few hours if dynamic groups or roles were in use.
SF-1103472 ACM-84436	AFX logs were not filtered as relevant to a request.
SF-1133285 ACM-85099	When a web service was assigned for a request, an error occurred when clicking on the default form under "Additional Information".
SF-1049128 ACM-79721	A change in property types, caused by change requests for accounts that generated revocation change requests for users, led to incomplete information for revocation that failed on fulfillment errors.
SF-1081182 ACM-83561	Change requests could be skipped by the processing workflow.
SF-1122086 ACM-84828	An automatically generated revocation request would fail when using a directory for an account.
SF-1189389 SF-1189398 SF-1189510 SF-1189404 ACM-88467 ACM-88468 ACM-88485 ACM-88477	The system did not generate change requests from violation remediation actions for revoked accounts when simultaneously revoking and giving exceptional access for multiple accounts that belonged to the same app role.
SF-1223556 ACM-90304	When reverting a pending account, an Oracle error "ORA-19279" prevented successful completion of the action. Also, restarting RSA Identity Governance and Lifecycle while some change requests were not finalized could result in the same Oracle error "ORA-19279" and prevent server initialization that resulted in users not being able to log in.
SF-1162322 SF-1171080 SF-1185324 ACM-75782	A change request could not be performed because it misnamed the account name for the requested entitlements.
SF-1156659 ACM-86562	The Entitlement View did not filter correctly as instructed by "Initial set of entitlements to show" when triggered by a request button.
SF-1193655 ACM-89679	If a user closes the browser or navigates away from the page using any function other than the cancel or back buttons, entries for pending accounts are left in T_AV_ ACCOUNTS.
SF-1286545 ACM-93599	A "Remove account to group" change request from a webservice did not set the affected users in the request information.
SF-1189546 ACM-92989	An added submission field did not appear in Additional Information while creating a Change Request for an application with groups.

Account Management

Issue	Description
SF-837790 SF-694892 SF-828508 SF-1044336 ACM-78326	An account template configured with additional account parameters failed to add those parameters to a created account.
SF-1104583 ACM-84929	Imported mapping that had been deleted and recollected from the account data collector source would create duplicate mapping.
SF-1109146 ACM-83939	If the names of created or pending accounts were changed during fulfillment, duplicate accounts formed for returning users with deleted accounts.
SF-1143132 ACM-85968	A pending account cancelled in the fulfillment phase still created an account if the name matched to a previously deleted account.
SF-1085269 ACM-83004	An account template for role and rule changes could be improperly mapped to a request form through a workaround.
SF-1147941 ACM-86123	The user interface did not allow users to remove pending accounts with names that were incorrectly entered.
SF-892981 SF-1103183 ACM-71073	The Who Has Access tab did not display any users.

Admin Errors

Issue	Description
SF-1223251 ACM-90384	A Notification rule that used Identity Unification as an error source did not send an email to the specified users as expected.
SF-1265089 ACM-92855	The Account Load Data error was not listed for available types in the properties of a Create Admin Error workflow node.

AFX

Issue	Description
SF-1046014 ACM-83743	When SOAP AFX connector had an external dependency, it failed to load WSDL over SSL or with basic authentication.
SF-1101671 ACM-83564	The AFX connector accepted and tested a password, but then failed to use it if the password was saved with "<" in the character string.
SF-1055876 SF-1123340 SF-1130377 ACM-80902	The Database Driver field for the SQLServer connector template did not appear after migration.
SF-1194056 ACM-88781	The maximum length of the JDBC URL field was too short for AFX connectors.

Issue	Description
SF-1064046 SF-1120246 ACM-84535	The Oracle Directory Server connector failed to create an account when the userPassword attribute was required for account creation.
SF-812176 SF-898611 ACM-64806	AFX command output parameters did not work if the attribute name contained a space.
ACM-63928	The afx_server getlogs command did not produce a gzipped file containing logs.
SF-897298 ACM-76107	After exporting an AFX connector with enabled capabilities, if the capabilities did not have any defined mappings, the capabilities were disabled upon import.
SF-936411 ACM-73373	AFX erroneously resent requests that had previously failed or been canceled.

Application Wizards

Issue	Description
SF-839184 ACM-67710	The Users count under Applications > General did not update after importing or updating the mapping.
SF-1142271 ACM-85633	Two or more users with the same name and different user IDs could not be added to a business unit's Other Business Owner field.

Authentication

Issue	Description
SF-856151 ACM-65647	Accessing an approval URL when logged in through SSO caused a NullPointerException error.
SF-1059226 ACM-84670	The Forgot Password feature did not work after a change in the user locale by the browser language settings.
SF-1215963 ACM-90219	The Active Directory objectGUID and objectSID were not properly supported attributes from authentication sources for either account or identity data collection.
SF-899125 ACM-71387	A null pointer exception occurred when parsing SAML responses.

Aveksa Statistics Report

Issue	Description
SF-1165448 SF-1170461 ACM-86990 ACM-90517	The ASR did not pull data for Web Application Machine Information.
SF-810446 SF-834464 SF-1078132 SF-1183919	A null pointer exception error occurred when creating an ASR with "Include database performance statistics" enabled.

Issue	Description
ACM-64920	

Change Requests and Workflows

Issue	Description
SF-1053443 ACM-83569	If Enable Email Reply Processing was unchecked and saved, then related options were not properly hidden.
SF-1101627 ACM-83545	A Delete Account change request could be marked as complete but still show a status of "Pending Action".
SF-1069608 ACM-81876	Manual Request Additional Info escalations could prevent an automatic Reassign to Supervisor escalation from running as expected.
SF-1104201 ACM-83552	The save button did not function properly when a resource, escalation, job variable, or webservice response was added, edited, or deleted.
SF-1022154 ACM-78550	A Change request generated using an unowned group and an owned group would incorrectly assign all of the change request items to the second group's owner for approval.
SF-4036115 ACM-82463	When generating a change request with users who had outstanding change requests, the generated change request incorrectly excluded any users who did not have an outstanding change request.
SF-1098925 ACM-83236	Imported legacy workflows created before version 7.0.1 had a legacy value not handled by the new architect editor.
SF-1110903 ACM-84016	The Provisioning Command node did not display job variables in the node properties.
SF-1118999 SF-1119764 ACM-84554 ACM-84218	A user access request with multiple entitlement changes did not reliably create account change items for adding entitlements depending on the order of selected actions.
SF-1143477 ACM-85731	After an upgrade, transition were not displayed in processing workflows that were created in the previous product version.
SF-684868 ACM-55740	After completing an activity, users could see all completed activity on the By Entitlement tab instead of just their own.
SF-1077691 ACM-81947	An exception error occurred when evaluating fulfillments with dynamic roles and group resources.
SF-1040676 ACM-79305	An entire change request would be rejected at the fulfillment phase if it had an entitlement deleted by a partial rejection in the approval phase.
SF-867542 ACM-74045	Activity nodes in a workflow were skipped if AFX fulfillment came back as Completed.
SF-929278 SF-1042033 SF-1063111	The Provisioning Command node did not save attribute values correctly when commas were used.

Issue	Description
ACM-73194	
SF-1138470 SF-1125576 ACM-86190 ACM-85810	Imported workflows could not send email after an upgrade because of email body errors and Send Email node errors.
SF-1116690 ACM-85129	SOAP and REST web service nodes could not be exited if the code window was expanded.
SF-1077035 SF-1146372 ACM-83585	Approval or Fulfillment nodes sometimes skipped when retrying after a concurrency error did not update the job with new node and sub-process data.
SF-1156274 ACM-86559	The workflow reference ID appeared for a subprocess instead of the workflow name when "Only show workflows similar to the current workflow" was checked.
SF-1045572 ACM-79675	The provisioning node mapping misaligned nodes when mapping a hardcoded value to a parameter value with a comma.
SF-1176466 SF-1181417 ACM-88269	AFX Requests with the "Entitlements Require Account" setting enabled would stall in the "Waiting for Dependencies" state.
SF-1083779 ACM-82500	Change requests with Joiner rules could experience a deadlock error caused by a Workpoint bug when the workflow is under a heavy load.
SF-1043713 SF-1148983 ACM-79531	Workflow variables containing multiple rows of data displayed with the comma delimiters.
SF-1192752 ACM-88582	Change request variables did not appear when fulfillment workflow edits updated the wrong variable.
SF-889452 ACM-71049	The default AFX manual fulfillment subprocess did not have a job state node to cancel change items, which caused change items in a canceled fulfillment to be stuck in "pending verification" status.
SF-1173926 ACM-88384	Custom workflows could not be deleted.
SF-981459 ACM-75938	Accounts and entitlements added through the "Complete Manual Activity Before Collection" feature would not appear in the user interface when referenced outside of the Users page.
SF-1152348 ACM-86911	When a Workpoint license check failed due to a connection issue, the user was required to restart the system or reload the license.
SF-1127411 ACM-86163	The workflow business calendar did not consider holiday hours when assigning due dates to workflow actions.
SF-1058844 ACM-83640	The **Show Job Level Variables** checkbox did not appear for Escalation workflows.
SF-1059087	Canceling a change request that added a role with entitlements or groups reverted the

Issue	Description
ACM-81419	role but did not remove indirect entitlements.
SF-1168903 ACM-89833	A change request generated from a termination rule bypassed a custom fulfillment workflow.
SF-1217300 ACM-89860	The URL parameter variables ${ValidReplyAnswers} and ${WorkItemURL} did not show in the workflow design page as available shortcuts.
SF-981092 ACM-84977	The decision node for workflow conditions on a request escalation was always set as "true".
SF-1181059 ACM-88351	The Show Job Level Variables setting in request workflows overwrote the same setting in approval and fulfillment workflows.
SF-1192314 ACM-90476	A custom task could not be deleted if it was scheduled.
SF-1204867 ACM-89649	When editing existing exceptional access, the user interface limited the business justification to 500 characters while it allowed 4000 characters for new entries.
SF-1258377 ACM-92069	After applying a patch, Workflow SQL nodes periodically failed with null pointer exceptions.
SF-01171991 ACM-88211	Non-Access Request workflows had inconsistent behavior dealing with Activities.
SF-1138522 ACM-85418	Decision Node settings changed automatically in the Out of Office workflow when any other node was changed and saved.
SF-1222578 ACM-90665	The variable value ${access_request_cri_app_cas2} did not successfully populate after a patch was applied.
SF-1158316 SF-1204062 ACM-90489 ACM-90603	Workflow variable names showed unexpected format changes after an upgrade.
SF-774980 ACM-66372	When a role is set as a resource for fulfillment, a member of the role could not use the Upload Attachment option.
SF-1266678 ACM-93462	The "Assign to" list incorrectly showed as an option for Resource Selection.
SF-1294015 ACM-94309	The Jobs tab in Admin > Workflow showed a UI error when evaluating errors with over 4000 characters.
SF-1304407 ACM-94532	A subprocess node condition applied to nodes without following configured settings.
SF-1297357 ACM-94126	The Group by Category approvals were skipped in Joiner workflows.
SF-1277724 ACM-92992	The REST Node POST request body mandated XML code that was not required.

Issue	Description
ACM-92993	
SF-1161187 ACM-90147	An Errors link in the run history of a Custom Task job summary table did not show the logged errors when clicked.
SF-1293969 ACM-94160	The AFX create account action failed when a change request with multiple "Create Account" items for multiple applications and for a single user has one of the "Create Account" items rejected.
SF-1281281 ACM-93288	Changes to customerstrings.properties did not reflect in the change request milestone display.

Collector

Issue	Description
SF-1110276 ACM-83742	Collection failed when the internal data file was larger than 2.15 gigabytes.
SF-964259 ACM-75432	A custom string attribute used for collection did not collect the LastLogonTimestamp attribute as expected.
SF-844956 SF-1087717 ACM-67283	Referrals were not ignored when "Ignore Referral" was checked in the connection settings.
SF-833758 SF-894036 ACM-66892	When an IDC collected the accountExpires date attribute from an Active Directory source, the time value varied on every collection based on the time zone.
SF-1116606 SF-1131797 ACM-84173	The ADC query test button reported an exception error.
SF-1164164 SF-1172536 ACM-86975	Multi-app collectors slowed down when older data was not removed as expected and instead accumulated with each run.
SF-1185812 ACM-88921	An LDAP search initiated by RSA Identity Governance and Lifecycle asked for the same AD attribute multiple times if it was mapped to more than one of the attributes for RSA Identity Governance and Lifecycle.
SF-1218345 ACM-90039	A new IDC for SQL Server could not locate the correct driver when selecting the DB Type.
SF-1190006 ACM-88607	When testing a role collector query, syntax errors occurred.
SF-1305102 ACM-94653	CSV database processing could not handle column header values nested in double quotation marks.
SF-1299910 ACM-94323	The Salesforce ADC was missing attributes listed in the datasheet.

Connector

Issue	Description
SF-953019 SF-1094710 ACM-74103	A line break character in search filters caused the test collection to fail for the LDAP collector.
SF-1111150 ACM-84090	After an upgrade, attribute synchronization on the AD connector applied the attribute_ sync prefix to non-empty & non-account variables, which updated values not required as well.
SF-976731 ACM-79126	Account template parameters did not correctly expand variables in password type attribute fields.
SF-1136239 ACM-85602	The Generic Database template with db2 type selected resulted in an error.
SF-1162980 ACM-87472	Active Directory attribute synchronization was unsuccessful in some environments when the account attribute values were set to null.
SF-894746 ACM-71014	The Active Directory AFX Connector could not set the PASSWD_CANT_CHANGE Active Directory attribute.
SF-1059478 ACM-80536	The SAP connector did not support the USERTYP account attribute.
SF-1202432 ACM-88958	When an AFX connector template and a connector had identical names, an error occurred when attempting to export the template and connector at the same time.
SF-1205499 SF-984004 SF-1051212 SF-836060 ACM-89197	After performing a migration, the Federated Salesforce connector template and Microsoft Exchange connector template remained in a migration required state.
SF-1214862 ACM-89813	The ServiceNow AFX Connector lacked command output parameter settings for the "Check Ticket Status" and "Check Request Status" capabilities.

Dashboard

Issue	Description
SF-1167801 ACM-87247	A custom user link in a dashboard appended "&width=null&height=null" to the URL, which caused some external pages to not load properly.
SF-1032894 ACM-80335	Dashboard links containing a query parameter that included a bind variable did not return the expected results.

Data Collection Processing and Management

Issue	Description
SF-1088219 ACM-82998	The IDC User Interface did not show whether the IDC required a Full Refresh.
SF-1104583	Pending User Account mapping and subsequent local mapping were removed every time the ADC ran collection.

Issue	Description
ACM-83603	
SF-1100515 ACM-83254	A collection that failed on the circuit breaker update did not remove the green check mark from the Last Successful Collection Date field.
SF-1063378 ACM-82700	After unmapping users from the accounts, the users sometimes erroneously retained access.
SF-1100498 ACM-83252	Procedures to purge older raw datasets caused circuit breaker failures when they erroneously purged raw datasets for collectors queued for processing.
ACM-53235	Internal data files such as STX tables and temporary data files in the server/default/deploy/aveksa.ear/aveksa.war/WEB-INF/AveksaDataDir directory were not removed as expected if the "Remove Internal Data Files After Upload" option was set to Yes.
SF-1068551 SF-930028 ACM-83338 ACM-73635	For users making role changes, role data collection would sometimes cause deadlocks due to database-stored procedures making unnecessary row updates to roles, even when they were not changed.
SF-596501 SF-714442 SF-820106 ACM-50485	Collection fails with an unclear error message when the collection source contains a special character that cannot be parsed.
SF-1115169 ACM-84129	Starting a unification run with migrated user records from before 7.x failed with "ORA-30926: unable to get a stable set of rows in the source tables" in 7.0.2 p2.
SF-1121551 SF-1128128 ACM-84547 ACM-84928	Unifying data with duplicate values caused failed collections with the message "ORA-30926: unable to get a stable set of rows in the source tables".
SF-1103183 ACM-84750	The "Who Has Access" tab for Data Resources was not populated after a long-running data collection by the primary DAC that was misidentified as secondary.
SF-1059311 ACM-83235	The DAG collector stalled after pre-processing a large data validation query.
SF-988361 ACM-83488	The account and entitlement data collectors did not collect user attributes CAS6 through CAS10 for indirect group entitlements.
SF-1133387 ACM-85100	The account and entitlement data collectors did not collect CAS user attributes in the correct order and could not properly assign the value of CAS10 as a result.
SF-1101593 ACM-83516	Unifications could fail due to improper clean-up of the tables used for prior data collections.
SF-1131773 ACM-85098	Unification sometimes assigned a deletion date for users that prevented them from logging in.
SF-1097757 SF-1119006	Temporary STX tables were left behind if the circuit breaker was triggered.

Issue	Description
SF-1042848 SF-1042140 SF-1114071 SF-1126989 SF-1077894 ACM-85534	
ACM-85488	User access to data resources could not be reviewed if assigned only through a group that was not properly tagged after data collection.
SF-1131077 ACM-85203	A sub-group to group membership was rejected because the name of the group had a space at the end that was not consistently trimmed at the source and when collected.
ACM-85608	Calculated totals for applications did not include group memberships as entitlements.
SF-1145208 ACM-86417	Role collectors aborted runs for groups that were role entitlements because of a case-insensitive search.
SF-934435 SF-1115169 SF-1113587 ACM-73247	Reused user_id attributes in an IDC caused unification with other IDCs to fail.
SF-1159109 ACM-86620	The DAG collector queries took many hours longer than expected to complete.
SF-1120976 ACM-86422	Collected subgroups from an LDAP were resolved as accounts instead of as groups.
SF-942302 ACM-74626	The Application Metadata Collector updated some non-application business source objects, such as role sets, in error.
SF-1160713 ACM-87431	User type attributes did not consistently appear for a unified user after a unification.
SF-1126909 SF-1185935 ACM-85023	Pressing Enter on the Forgot Password screen canceled the process.
SF-1166339 ACM-88505	After the ADC ran, the Foreign Security Principal (FSP) membership changes in Active Directory did not update in RSA Identity Governance and Lifecycle.
SF-1165478 ACM-87066	Unification sometimes terminated users and duplicated them into new User IDs.
SF-981459 ACM-75980	Accounts and entitlements added through the "Complete Manual Activity Before Collection" feature were not reconciled or removed after running collection.
SF-1176684 ACM-87842	Performance issues occurred for indirect relationship processing when processing deleted role relationships.
SF-1193983 ACM-88706	The Role Data Collector failed with an Oracle error that reported unstable rows in the source tables.

Issue	Description
SF-1213227 ACM-89674	The Account Data Collector could not call custom code prior to loading the raw data.
SF-1197266 ACM-88960	Any unprivileged user could export or save data in a table displayed within a pop-up.
SF-1220029 ACM-90277	Manually mapping a user account submitted a new indirect relationship processing job whether or not the job was already in queue.
SF-1062777 SF-1020344 SF-1108676 SF-1213238 SF-1224190 SF-1219428 ACM-81403	Group collection rejected the nested group relationships and misidentified groups as accounts when listed as members of other groups.
SF-1175678 ACM-87948	Collections from a .csv file returned too many rows after an upgrade.
SF-1224169 ACM-91121	Collection added duplicate Aveksa access entitlements to the account and user.
SF-1228554 ACM-90663	A data table stored historical configuration information in clear text.
SF-1201069 ACM-89785	Duplicates created in the T_SCHEDULED_TASKS table prevented unification from completing.
SF-1058100 ACM-80563	When a user was moved from one IDC to another, unification terminated the original user and created a duplicate user.
SF-1260229 ACM-92496	Unification failed with unknown error after an upgrade.
SF-1242815 ACM-91761	The Last Reviewed Date OOTB attribute erroneously showed as an available collector mapping attribute in the UI.
SF-1300333 ACM-94263	Running two MAEDCs failed with error ORA-30926 if they overlapped in applications and IDs.
SF-1312022 ACM-93036	The App Metadata collector failed with the "character string buffer too small" error.
SF-1236885 ACM-91586	An ADC User Resolution with more than 3 attributes from the same source left an account unmapped and without an ORPHANED_DATE value.
SF-1231311 ACM-91584	Unification removed user account mapping when one of many resolution attributes was changed.

Database Management/Performance

Issue	Description
SF-01123301	Data archiving had a processing failure.

Issue	Description
ACM-84609	
SF-1150006 ACM-86789	The GATHER_DATABASE_STATISTICS task failed on a buffer overflow error.
SF-1164598 ACM-86987	The database slowed, reported multiple errors, and then used up all resources when conducting bulk reviews on thousands of items.
ACM-90149	A backup started with a backup already in progress stopped with a warning but did not return with a failed status.
SF-1164598 ACM-88699	Illegal TXN State errors were reported in the user interface after applying a patch.
SF-892279 SF-1068981 SF-1186911 ACM-72284	The PV_USER_DIRECT_ACCESS view did not have a join condition on the entitled ID to show correct information.
SF-1190864 SF-1190863 ACM-88534	Slow SQL query performance occurred after upgrading from version 6.9.1.
SF-1224207 ACM-90323	A Data purge job that ran through the backend repeatedly failed to complete the custom task purge.
SF-1201744 ACM-89849	Performance issues occurred when revoking entitlements from a role during a fine-grained role review.
SF-1074740 ACM-85409	An error occurred after a CLOB was converted into a varchar in the CHANGE_REQUEST_VARIABLE view.
SF-1203774 ACM-88976	Performance issues occurred when editing roles.
SF-1110258 ACM-87245	When the database unexpectedly shut down, ACM and AFX continued to run but did not function after the database was started.
SF-1128305 ACM-85934	User interface page-loading time and collections took an unusually long time.
SF-1312843 SF-1298331 ACM-94891	Rule pre-processing performance significantly slowed after adding segregation-of-duty rules for a large environment.

Descriptions

Issue	Description
SF-1209242 ACM-89625	During the import of business descriptions, the status pop-up that appears when importing business descriptions did not appear when choosing to overwrite or skip existing entries.

Email

Issue	Description
SF-1067879 SF-1069696 SF-1134843 ACM-81341	If the special character % was in the e-mail content, then the email could not be generated.
SF-1039470 ACM-79253	Emails generated for exported reports incorrectly capitalized the report file extension.
SF-1086751 ACM-83216	Email processing failed and displayed the error "Wrong user replied" for approvals sent to dynamically assigned approvers in a role.
SF-1136705 ACM-85359	Escalation emails were not updating the value used by the runtime to send with proper priority.
SF-1004034 ACM-80529	A Review Reminder email configured for 24-hour intervals generated at 12-hour intervals instead.
SF-1162253 ACM-86909	Security access request approval email links did not work.
SF-1038728 ACM-79982	The user interface became unresponsive when an emailed tabular report bounced due to size limitations of the recipient's mailbox server and the aveksaServer.log file recorded the email along with the entire attachment in encrypted format.
SF-978800 SF-1131929 ACM-75696	Email server configuration needed to allow for separate authentication configuration for inbound and outbound servers.
SF-1056837 SF-1155367 ACM-80572	A requestor still received approval emails despite being on the Exclude list.

Installer

Issue	Description
SF-970037 SF-1108073 ACM-76001	Aveksa.ear contained duplicate files that caused zip errors during deployment.
SF-1141841 ACM-86014	A supported database version could not be confirmed during migration.
SF-1137353 SF-1142351 SF-1138013 ACM-85438	The installer checked for unneeded packages and caused installation in a WildFly environment to fail.
SF-1115317 ACM-84107	A typo appeared in the installOracle.sh script.
SF-1129043 SF-1139113	Installation or upgrade on Red Hat 6.5 and 6.8 failed when IPv6 was disabled.

Issue	Description
SF-1136656 ACM-85437	
SF-1130896 SF-1139955 SF-1150455 ACM-85021	The aveksaWFArchitect.ear file could not be deployed on WebLogic 12.2.1.3.0 due to a conflict in the Java Spring-Boot library.
SF-1150455 SF-1176964 ACM-86894	A schema could not be created or migrated when using non-default tablespace names.
SF-1182857 ACM-88297	Schema patching errors occurred when upgrading a WebSphere installation.
SF-1166648 ACM-87123	After patching RSA Identity Governance and Lifecycle, the user interface did not display an Edit button for the Email Fulfillment Handler as expected.
SF-1193541 ACM-88761	The oracle error "ORA-30657: operation not supported on external organized table" occurred when applying an upgrade or patch.
SF-973587 ACM-75344	The Patch installation process did not stop to show an error message when an issue occurred with the archived .ear file.
SF-1205479 ACM-89296	The Database-Only installation did not check for sufficient disk space to complete installation.
SF-1189209 ACM-89224	In a database-only installation, the installer does not check resolv.conf for prerequisites.
SF-942673 ACM-73935	The installation or upgrade process would get stuck when one or more required install packages were missing.

Metadata Import/Export

Issue	Description
ACM-84989	Metadata sometimes exported with random, duplicated objects on subsequent attempts after the first export.
SF-1077965 ACM-82017	Incorrect error message was displayed when importing a rule with an invalid global role reference.

Migration

Issue	Description
SF-1220848 SF-1222279 SF-1226660 ACM-90260 ACM-90607 ACM-90220	The ViewPasswordUrl setting in the t_system_settings table failed to update when using the oracle dbms_lob utility with a large customerstring.properties file.

Password Management

Issue	Description
SF-1069908 ACM-81479	Password validation did not work consistently from the user interface and from an external password reset link.
SF-1022835 ACM-79684	The process to add or change a password policy to an application stalled when table views accessed a very large number of records.
SF-1173793 ACM-88150	The current password could not be validated against a stored password history hash during a password change.

Provisioning

Issue	Description
SF-1192284 ACM-88777	The Workflow ValidReplyAnswers macro did not populate and list URLs in a consistent order.

Reports

Issue	Description
SF-1004352 ACM-79058	A new chart could not be created with the same name as an existing tabular report.
SF-1043556 ACM-81849	The / character in a report file name created a report schedule that failed if the option to send attachments was enabled.
SF-826817 ACM-67195	Reports exported using the .xls file extension were not properly formatted.
SF-1101300 ACM-83537	Reports exported to an Excel spreadsheet did not restore a previously deleted temporary folder and, as a result, returned blank rows instead of the expected data.
SF-767212 SF-824328 ACM-60522	After upgrading, reports containing Cyrillic characters still did not display correctly when exported as .xls or .csv filetypes.
SF-838887 ACM-71716	The report template "Entitlement Review Item Details by Reviewer" did not display the custom review state.
SF-01143644 ACM-85658	The order of the list columns available in the Report Column tab changed randomly.
SF-647482 ACM-52763	Imported Custom Report templates copied unnecessary attributes that caused errors.
SF-949068 ACM-76876	Reports exported into the CSV or XLS format occasionally did not retain any data.
SF-882602 ACM-71754	An Out of Role Entitlements report did not show the expected results.
SF-1219878 ACM-90510	The T_AV_AFX_LOG_MESSAGE and T_EMAIL_LOG tables lacked a public view of their data.

Issue	Description
ACM-90511	
SF-1271093 ACM-92667	Scheduled reports in XLS-format could not be opened after migration.
SF-1258049 ACM-92226	After an upgrade, reports using the PV_USER_ALL_ACCESS view failed with an error if the report had custom value integer attributes.
SF-782401 ACM-63770	After applying a style template to a report or report template, the Apply Style Template to Report screen did not indicate the currently applied style.
SF-729074 ACM-56680	The Review Item Details Report could not be filtered using the Status attribute.
SF-1219878 ACM-90512	The tables T_AV_AFX_REQUEST & T_AV_AFX_REQUEST_HISTORY did not contain public views.
SF-1130030 ACM-88494	A Report with a non-standard column defined with TO_DATE/TO_TIMESTAMP functions in a select statement could fail to extract the date and showed the "jasperreports.engine.JRRuntimeException" error instead.
SF-1174014 ACM-87747	The OOTB "Leavers or Terminated Users" report did not show deleted users as expected.

Request Forms

Issue	Description
SF-1025815 ACM-82420	The validation URL did not work for the "Drop Down Select from Web Service" control type.
SF-1084223 ACM-82486	The form tooltip for tables did not display when added to a question.
SF-1059905 ACM-82742	A question with a multi-select drop-down control did not trigger a display condition tied to selecting a drop-down option unless the same condition was also assigned to a secondary control.
SF-992540 ACM-76461	Forms did not display terminated users when a custom form or form list was opened by a request button action.
SF-1065124 ACM-81155	On request and approval forms, when using a submission question with a Select Drop Down list, only the first value was used.
SF-792046 ACM-65018	Non-visual entitlement tables were displayed on a submitted request form.
SF-1112926 ACM-85657	Out-of-the-box Application Business Source attributes returned null values when called through variables in request forms.
SF-931948 ACM-74069	An entitlement table field on an existing request form with a "Show child entitlements of" attribute did not retain its value when copied to a new request form.
SF-1013039 ACM-77523	An option in a Drop Down Select control could not be deleted if the user put single quotation marks around the value.
SF-1143371	The text area field was not validated for the maximum character limit if the related

Issue	Description
ACM-85654	question had an apostrophe.
SF-1109812 ACM-83706	The Drop Down Select control type for request forms was not disabled as intended if Enable conditions were set.
SF-1094196 ACM-83637	In request forms, the Display and Enable conditions for the Javascript field in request forms did not work as expected.
SF-968958 ACM-76010	The "Allow Multiple Selections" setting did not work correctly in a User Account Table field in a form.
SF-1100787 ACM-84628	Custom dropdowns did not retain selections with web service fields.
SF-1127904 ACM-85244	A request form did not handle user details containing "\" properly for user pickers and the provisioning command.
SF-840034 SF-999420 ACM-67318	A request form did not show the correct entry when an apostrophe is present in the value of a variable.
SF-1097313 ACM-83168	The selected value for a radio button appeared as ??? when passed to other form controls through the avform variable.
SF-815680 ACM-64863	Request forms allowed users to move to the next page before all the form fields had finished loading.
SF-1131084 ACM-85886	Child entitlements of pre-selected entitlements did not load in an entitlement table form control.
SF-960379 ACM-74603	Form text fields with a long entry did not show the complete text in request or approval screens.
SF-1168573 ACM-87946	The password generator URI field did not resolve form variables.
SF-1151669 ACM-86387	A warning message on change requests needed clarification.
SF-1184989 SF-1179125 ACM-88383 ACM-88439	After changing the value of an avform variable, related form controls with display conditions did not update.
SF-1889550 ACM-88604	Multiple account resolution prompts for every entitlement change created as account changes could lead to excessive prompts.
SF-887157 SF-957895 SF-1002780 ACM-70736	User filters with avform.user variables added to the Compare Users field of the Provisioning form removed all users instead.
SF-1038696 ACM-79773	The form did not correctly show certain colors to highlight target users depending on their access.

Issue	Description
SF-1210320 ACM-89468	When Multiple Account Resolution is set to "per business source" and the request form adds entitlements from multiple applications that are tied to the same underlying directory, account prompts appear for each application instead of once for the directory.
SF-1188323 ACM-88507	When the User Selection screen for an Access Request form has a grouping that contains more than 100,000 users, the following error occurred when expanding and collapsing the grouping: "Error - java.land.IndexOutOfBoundsException: Index: 100000, Size: 100000".
SF-1194256 ACM-88878	The Display and Enabled conditions for an entitlement table did not work as expected.
SF-1239355 ACM-91122	The conditions to display or enable an entitlement table form control could not be properly verified in the form.
SF-912473 SF-957890 ACM-72112	The request form did not properly validate a direct request for entitlements that were already granted indirectly through a role.
SF-1086944 ACM-83740	Multiple entitlement tables that used Display conditions, Enable conditions, and Form variables in their entitlement rules sometimes displayed improperly.
SF-1263329 ACM-92257	A request form associated with a business source could not be edited because of an error.
SF-1212317 ACM-90015	Email sent with an External URL link that contains the externalURL and title parameters caused "request could not be handled" errors.
SF-968478 ACM-76164	When a form was designed with an application name that did not match the business source raw name, the account filter did not work correctly.
SF-1212748 ACM-91669	The entitlement table with display conditions did not appear when the dynamic variable value changed.

Role Management

Issue	Description
SF-1069369 ACM-81602	The user interface for coarse-grained role reviews provided options to remove or edit members and entitlements, even though coarse-grained role reviews are intended for high-level review and not to make individual changes.
SF-817316 SF-844023 ACM-65297	Custom attributes created with the same name but assigned to different entitlement types appeared identical and did not work correctly when setting an entitlement rule in a role set.
SF-1142958 ACM-85634	A Null pointer exception error occurred when creating a new role while logged in as the business role owner of a role set.
SF-1112926 ACM-85657	Out-of-the-box Application Business Source attributes returned null values when called through variables in request forms.
SF-1149895 SF-1083679	Fixes to the role set persistence of a role caused problems with entitlements when there were role set changes.

Issue	Description
SF-1123786 ACM-86112 ACM-83273	
SF-1078256 ACM-82957	After importing a modified XML file of existing global roles, the Long Description was not updated.
SF-839546 ACM-66820	A new role with no members or entitlements did not appear in search results when the search filter was set with the member or entitlement count as zero.
SF-22039 ACM-48746	The Request Hierarchy Children entitlement selector allowed selected entitlements to exceed the actual total.
SF-1071138 ACM-74902	The error "Unable to find RoleSet ID" appeared in logs while creating a role collector with the raw name and alt name roleset attributes as different entries.
SF-963152 ACM-63734 ACM-75430	Collected roles that were exported did not fully import when imported into same environment.
SF-1067111 ACM-66489	When a change request removed a child technical role from a parent business role, it also erroneously removed group entitlements that were shared from a different child technical role with common entitlements.
SF-1190065 ACM-88496	The user interface did not display a role in a role set due to a query error.
SF-1113010 ACM-84589	The displayed number of suggestions and violations did not correctly update collection when membership rules changed for a role and the role moved to the pending state.
SF-1089845 ACM-85357	The Role analytics table for missing required entitlements incorrectly showed technical roles as global roles.
SF-911444 ACM-77583	Terminated users were erroneously granted indirect role memberships when they were still part of a role that added an entitlement.
SF-927983 ACM-73210	Role Discovery stalled and timed out on a database query when using a high-load HASH-JOIN view on the GTT_CLUSTER_ENT_COUNTS table.
SF-901924 ACM-73623	A specific role showed a "could not execute query" error in the user interface instead of the role data.
SF-1213844 ACM-90265	A null pointer exception error occurred when viewing the Out of Constraints users section in Analytics if "Remove" is the only column in the table.
SF-1166227 ACM-87106	On the Analytics tab, the Out of constraint user table disappeared and the UI locked up and displayed incorrectly when a user was removed from the table.
SF-1089845 SF-1132001 ACM-84396	Cascaded roles were missing to be added as entitlements while creating a change request from the Role Missing Entitlements rule execution.
SF-950510 ACM-74637	The "Role Missing Entitlement Rule" email notification did not include the group entitlement collected from ADC. Code was missing to add the group entitlement to the

Issue	Description
	email notifications.
SF-882193 ACM-70716	When creating roles using the Discover Roles functionality, the suggested entitlements do not match the suggested entitlements condition.

Rules

Issue	Description
SF-1095861 ACM-83120	When a change request was created by a role change, decision Nodes ignored the "Contains at least one violation" condition.
SF-1052613 ACM-84945	When the Attribute Change rule for Managed Attributes used the "Set to old value of" argument, the rule sometimes failed to set values after the first user matched by the rule.
SF-1120488 ACM-84536	During access request creation, when a user views the Accounts selection screen and then goes back to the previous screens to make changes, violations by the new changes were sometimes not displayed.
SF-1127651 ACM-84810	Out-of-the-box workflow form controls were listed in the Violation Remediation node that did not work for the node.
SF-1114903 ACM-83574	Changing the User Access/Separation of Duty Rule definition closed some violations but left their remediation workflows active.
ACM-83212	New violations could incorrectly be added to existing remediation workflows, when a new workflow was necessary.
SF-1105975 ACM-83937	The number of violations did not appear correctly in the status column.
SF-1057748 SF-1125122 ACM-84105	The user interface did not display violations that were not in sync with the remediation workflow to remediators.
SF-1125118 ACM-84592	A rule violation remained in Pending Revocation status after rejection of a corresponding change request item.
SF-1121216 ACM-84791	A condition for access containing IN for a rules definition could not be re-edited for attributes with case-insensitive "name" in the label.
SF-774383 ACM-63346	After migration, violations appeared with the wrong state.
SF-1139602 ACM-85892	After modifying a collector, a UCD rule detected changes that had already been validated following a previous detection.
SF-1169066 ACM-87411	Provisioning Termination and Attribute Sync rules incorrectly processed local user mapping for pending accounts.
SF-1147687 ACM-87267	Renaming a Notification Rule left an orphaned item in the scheduled tasks for that rule.
SF-1180940 ACM-88634	A Termination Rule with the 'or' condition for a Delete Accounts action did not create the expected change requests to revoke entitlements.

Issue	Description
SF-1080104 SF-642932 ACM-52576	The termination rule created a duplicate request that could not be completed when a user was terminated and then deleted.
SF-1208949 ACM-90043	Detected violations did not associate with remediation workflow jobs during rule processing due to an Oracle buffer overflow error.
SF-1000621 SF-1041352 SF-1100872 ACM-77042	Scheduled rules ran multiple times when the rule name or type had been changed.
SF-1025263 SF-1026091 SF-1073300 SF-1126913 ACM-78589	Change requests created by an unauthorized change detection rule identified the wrong user in the details.
SF-1262986 ACM-92256	Violation detection information on the User Request Details page worked only when a User Access Rule was configured with a single user for all entitlements scenario.
SF-1101217 ACM-83760	An Out of Memory error occurred while processing a large number of Role Membership Rule Difference rules.
ACM-95300	Rules processing failed with Oracle error ORA-01652 when all rules were processed simultaneously.

Security

Issue	Description
SF-1095483 ACM-84155	Applied security fixes for workflow editor properties.
SF-940772 SF-1174388 ACM-73739	Users could access pages in RSA Identity Governance and Lifecycle without required privileges.
SF-1213459 ACM-90322	The patch includes an updated version of JDK 8, which addresses some known security vulnerabilities.
SF-1087041 ACM-83001	A bind mount of the /var/tmp directory to the /tmp directory was needed in hardware appliance deployments.
SF-1215126 ACM-90300	Users were able to edit the sender’s email address in the Send Email to Users form for reviews if permitted by the review definition. The setting that allows the sender's email address to be changed has been deprecated.
SF-1087041 ACM-83000	The setDeployEnv.sh script added a . to the root $PATH.
SF-1223436 ACM-91372	Users granted the "View All" role could not see group and role members in the What Access tab.
SF-1022650	Applied properties to enhance security for an internal communications port used by a

Issue	Description
ACM-78259	mule agent.

Server Core

Issue	Description
SF-903632 ACM-71675	A domain controller node in a hardware appliance with a local database could not stop, start, restart, or status-check the database using the aveksa_cluster script.
SF-1128205 SF-1144286 SF-1159804 ACM-84894	Heavy change request activity increased the ADC processing time for longer than expected.
SF-1061884 SF-1197693 ACM-83205	Scheduled and manually initiated tasks required improved handling and diagnostics.

User Interface

Issue	Description
SF-596472 ACM-51112	When editing review definitions, the Allow Expiration and Comments are Required checkboxes were cleared if the user switched tabs.
SF-843449 SF-931419 SF-932453 ACM-67243	Logging out led to a blank screen if confirmations for logging out were disabled.
SF-791436 ACM-62724	After adjusting table options, some columns did not display as configured when switching from a Group review result to a User review result.
SF-1001038 ACM-77791	The Max Users Per Change Request setting in Access Configuration disappeared from the Settings tab if not assigned a value.
ACM-84410	Performance issues occurred on the General tab of a role set after applying entitlement and membership rules.
SF-884453 SF-884449 SF-936962 SF-982809 SF-1084195 ACM-73706	Heartbeats, which help to avoid server timeouts when using forms and the Architect workflow editor, generated benign errors in the server log.
SF-1127021 SF-1149655 SF-1152703 SF-1149987 ACM-85554	Changes in the customerstrings.properties file were not saved after an application server restart.
SF-768669 ACM-65157	A truncated file size limit error was displayed for the attachments control type when using Internet Explorer.

Issue	Description
SF-830319 ACM-66283	The Owner attribute did not appear in the table options of the What Access tab under Resources.
SF-620510 ACM-52883	Underscores and spaces incorrectly replaced Hebrew characters in the user interface.
SF-1086944 ACM-85029	Performance issues occurred on the General tab of a role set after applying entitlement and membership rules.
SF-19207 SF-684770 ACM-45115	The date in the European format of DD/MM/YYYY did not properly appear for the English (UK) locale.
SF-904694 SF-873589 SF-1156305 ACM-72163	Benign errors appeared when a web service authenticated the AveksaAdmin user when no Aveksa system authentication source was defined for AveksaAdmin.
SF-1065497 ACM-81449	An invalid identifier error in request forms appeared when using the Other type for owners in a business source filter.
SF-1152397 ACM-86298	Clicking the Back button in the web browser did not load the previous page.
SF-954920 ACM-87252	Different security context configurations in the same .csv file did not work as expected.
SF-1073714 ACM-81669	After changing the name of a business unit, the user interface showed the old business unit name when grouping users by business unit.
SF-913568 ACM-75393	The User Change data table still showed the User ID field when not selected as a displayed column in Table Options.
SF-612632 ACM-51311	The What Access tab did not disable the filter to show pending entitlements when switching to another application.
SF-1158799 ACM-86788	The Accounts table in the Directories Resource Accounts Tab showed a "Backup Supervisor" column in Table Options that is never populated in an accounts table.
SF-1072223 SF-1080714 ACM-83584	Multiple clicks on a form could select one item multiple times to create duplicate selections.
SF-967960 ACM-76184 ACM-76185	Attributes did not display when searching in the Business Units or Application list.
SF-969882 ACM-75372	The notification button opened a blank window with a disabled Complete button if no tasks were available to the user.
SF-1178116 ACM-87998	The user interface did not properly display the long description for an application.
SF-1110294	The unique_ID attribute was not displayed on the summary page after changing the

Issue	Description
ACM-85141	language under user options.
SF-1104724 ACM-84228	Extended user attributes were not displayed on the summary page after changing the language under user options.
SF-1176345 ACM-88381	The node filter in System > Logs could not show any logs in a WebLogic environment.
SF-1042710 ACM-79980	The log page in Admin > Email did not show results correctly when sorted by Processing Result.
SF-1233063 ACM-91269	The database view V_ROLE_TO_APPS did not include local roles in addition to collected roles.
SF-1257307 ACM-93514	The UI became unresponsive when using French language settings.
SF-947231 ACM-75230	Disabled accounts on the Submit Request > Available Accounts page were not crossed out.

Web Services

Issue	Description
SF-1035349 ACM-81967	Web service requests did not show affected users.
SF-1253334 ACM-92041	Duplicate group names on a multi app collector could cause the webservice call that created a change request to choose the wrong group.
SF-1264262 ACM-92518	The documentation for the processRule Web Service did not state that a token was mandatory.

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-95827	In a WildFly environment, during the upgrade to RSA Identity Governance and Lifecycle 7.1.1 from version 7.1, the following message appears in the logs: "Initialization has failed! Database version is newer than product version. Cannot migrate newer databases to older versions." This error, which only appears in the logs, does not affect the actual upgrade process, and the upgrade completes successfully.
ACM-92819	In an environment using an external remote agent, the firewall blocks certificates generated by RSA Identity Governance and Lifecycle due to being non-compliant with RFC-5280. **Workaround:** Create an exception in the firewall to allow the certificates signed by the RSA CA.
ACM-87534	The warning message "Days value should not be blank" erroneously appears if the date

Tracking ID	Description
	range is set to "All" but the number of days in the unselected option is left blank. **Workaround**: Leave a numeric value greater than 0 in the Days field.
ACM-88135	The Log Artifact Collector cannot collect AFX logs from a remote AFX server. **Workaround**: Manually gather the remote AFX logs using the getlogs command after logging into the remote server.
ACM-89764	The Log Artifact Collector cannot collect database logs from a WebLogic environment with a remote database.
ACM-89840	The Log Artifact Collector collects empty log files when the date range for .zip file generation is set to "All".
ACM-90320	The Log Artifact Collector may not correctly locate the Oracle Alert logs on a WebSphere server with a local database. **Workaround**: Manually gather the Oracle alert logs from the database server.
ACM-92990	In a WildFly environment, JAAS configuration is not properly preserved when an authentication source is not created on the domain controller node. **Workaround**: Create authentication sources only on the domain controller node in a WildFly environment.

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;
/
```