RSA® Identity Governance and Lifecycle

V7.0.2 Patch 3
Release Notes

RSA

Contents

Install a Patch

The following procedures describe how to download and apply a patch to RSA Identity Governance and Lifecycle appliance and soft-appliance installations, and how to upgrade Access Fulfillment Express (AFX) connectors. Patches are cumulative.

Important: Do not attempt to install a previous version of a patch over a later version of a patch.

Before You Begin

- As of 7.0.2 Patch 2, the way in which RSA Identity Governance and Lifecycle handles business descriptions for groups has changed.

  Important: If your RSA Identity Governance and Lifecycle deployment includes business descriptions for groups, run the pre-migration queries for group business descriptions to identify any business descriptions that will be automatically deleted during the update process. For more information and the queries, see Migration Queries for Group Business Descriptions.

- If your environment uses a remote customer-supplied database, ensure that no database procedures are running against the database schema during the patch installation. The patch process may run SQL against various tables in the database.

  Note: On an appliance with a local, RSA-supplied database, the patch script automatically stops and starts the local database to ensure that this requirement is met.

- In a clustered environment, use only one node during the patch update process. Stop all other nodes in the cluster to ensure that multiple nodes do not attempt a database migration. Before you patch additional nodes or enable farming to push EAR changes to other nodes, validate that the patch is applied and the one node is working as expected.

- When upgrading from product versions older than 7.0.2, in all environments, you must upgrade to the base version 7.0.2 before installing any 7.0.2 patches.

Migration Queries for Group Business Descriptions

Important: 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;

/
```

Install the RSA Identity Governance and Lifecycle Patch

Use this procedure to install the patch on appliance and soft-appliance installations.

Procedure

1. If you have Access Fulfillment Express (AFX) installed, using the AFX user account, shut down all AFX instances before installing the patch upgrade:

   `<path-to-AFX_installation-directory>/AFX/afx stop`

2. To download the upgrade files:

   a. Log in to RSA Link, and click RSA Identity Governance and Lifecycle.

   b. Click **Downloads** > **RSA Identity Governance and Lifecycle *<Version>***, where *<Version>* is the version number of the product that you are patching.

   c. Click **Version Upgrades**.

   d. Click the **Upgrade** link for your licensed RSA Identity Governance and Lifecycle asset.

   e. Click **Continue**.

   f. On the Order Detail page, click the menu icon and select **Product List**.
      The **Current** tab provides the most current release or patch, and the **Archive** tab provides previous patches and releases.

   g. Click the appropriate tab, and select the name of the patch to download.

   h. Download the following files:
      Aveksa_*<VersionNumber>*_P*<PatchNumber>*.tar.gz

      upgradeJDK*<version>*_*<revision>*.tar (optional JDK update for security updates)

3. (Optional) To apply the JDK upgrade, do the following:

   a. Change to the Oracle directory: `cd /home/oracle`

   b. Decompress the file: `tar vxf upgradeJDK<version>_<revision>.tar`

   c. Log in as root, and run the following commands:

      i. `cd /home/oracle/upgradeJDK<version>_<revision>`

      ii. `chmod 777 *`

      iii. `cd deploy/`

      iv. `chmod 777 *`

      v. `cd ..`

      vi. `sh upgradeJDK<version>_<revision>.sh`

4. To decompress the patch file, Aveksa_<*VersionNumber*>_P<*PatchNumber*>.tar.gz, run the following commands:

   a. `cd /home/oracle`

   b. `tar zvxf Aveksa_<VersionNumber>_P<PatchNumber>.tar.gz`

5. Log in as root and run the patch.sh installation script in the directory created in Step 4. Run the following commands:

   a. `cd /home/oracle/Aveksa_<VersionNumber>_P<PatchNumber>`

   b. `sh patch.sh`

6. When the patch script completes, restart RSA Identity Governance and Lifecycle. Run the following command:

   `acm restart`

After You Finish

Important: Installing a patch overwrites all custom configuration settings. You must manually restore the settings after the import.

- In a WebSphere environment, after you deploy the patch, you must restart RSA Identity Governance and Lifecycle. When you start RSA Identity Governance and Lifecycle after applying the patch, SQL processing is performed. After SQL processing is complete, restart RSA Identity Governance and Lifecycle again, to ensure that any patch processing takes effect.
To stop and restart RSA Identity Governance and Lifecycle on a WebSphere server:

  1. In the WebSphere console, go to **Applications**.

  2. Under All Applications, select **aveksa**.

  3. Click **Stop** to stop the RSA Identity Governance and Lifecycle.

  4. After the aveksa application has been stopped, click **Start** to start RSA Identity Governance and Lifecycle.

- In a WebLogic environment, you must restart RSA Identity Governance and Lifecycle after you install the patch. For instructions, see the *RSA Identity Governance and Lifecycle Installation Guide*.

- If your deployment includes Access Fulfillment Express (AFX), you must also upgrade your AFX connectors. For instructions, see Download and Import AFX Connector Packages.

Download and Import AFX Connector Packages

If your RSA Identity Governance and Lifecycle deployment uses Access Fulfillment Express (AFX), use this procedure to download and import the AFX connector package. Reference the instructions in Step 2 above for accessing the software from RSA Link. In this case, look for an AFX link from Version Upgrades.

Procedure

1. Download the Connector package files to a directory local to the browser client from which you plan to import the packages:

   - AFX-<*Product_Version*>-Standard-Connectors.zip

   - AFX-<*Product_Version*>-Premium-Connectors.zip (SAP customers only)

2. Log on to RSA Identity Governance and Lifecycle.

3. Click **AFX > Import**.

4. Import the packages.

5. Run the following command:

   ```
   <path-to-AFX_installation-directory>/AFX/afx start
   ```

Release 7.0.2 Patch 3

Information about the 7.0.2 Patch 3 release is included in the following sections:

-
-
-

What's New in Release 7.0.2 Patch 3

Feature	What's New
Change Requests and Workflow	The workflow editor has been updated to Workpoint 4.4.0 Patch 10

User Interface Changes in Release 7.0.2 Patch 3

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
ACM-76598	Filename validation has been added for connectors and connector templates. The following characters are not allowed in filenames: \ / : * ? " < > |

Fixed Issues in 7.0.2 Patch 3

The following issues were fixed in 7.0.2 Patch 3.

Change Requests and Workflows

Issue	Description
SF-820520 ACM-66029	Duplicate 'remove' change items appeared from a request to remove a role from a user that had duplicated entitlements.
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	Importing a workflow with the overwrite option did not update the workflow

Issue	Description
ACM-72817	name.
SF-997361 ACM-77724	Conversions of decision nodes did not succeed unless performed during a patch upgrade.
SF-992247 ACM-76647	A rejected change request approval did not display after completing the workflow.

Collector

Issue	Description
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.
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-964094 ACM-76458	After installing RSA Identity Governance and Lifecycle, the identity collector would not connect to Novell IDM.

Custom Attributes

Issue	Description
SF-990118 ACM-76648	The PV_USERS view did not update with new custom user attributes.

Data Collection Processing and Management

Issue	Description
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.

Issue	Description
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-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.

Database Management/Performance

Issue	Description
SF-968303 ACM-75048	Exporting the activity table could cause "Out of Memory" errors when there was a large amount of activity data.

Email

Issue	Description
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.

Installer

Issue	Description
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.

Password Management

Issue	Description
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.

Reports

Issue	Description
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 SF-916311 ACM-63502	Filter criteria did not save when switching between the Query tab and the Filter Criteria tab.

Request Forms

Issue	Description
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.

Issue	Description
SF-984592 ACM-76631	Non-visual entitlement and account management tables incorrectly handled the shopping cart functionality.

Role Management

Issue	Description
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.

Web Services

Issue	Description
SF-981603 ACM-76590	A request to create an account from a Web service did not succeed when only one parameter was used.

Release 7.0.2 Patch 2

Information about the 7.0.2 Patch 2 release is included in the following sections:

- What's New in Release 7.0.2 Patch 2

- User Interface Changes in Release 7.0.2 Patch 2

- Fixed Issues in 7.0.2 Patch 2

- Known Issues in Release 7.0.2 Patch 2

What's New in Release 7.0.2 Patch 2

Feature	What's New
AveksaAdmin Password Security	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.
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. 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.

Feature	What's New
	• 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.
Platform	Upgraded OpenJDK to version 141 to provide the latest patches and security vulnerability fixes.
Reports	The Additional System Information section of the Aveksa Statistic Report (ASR) now includes a list of any custom files that have been uploaded.
Role Management	RSA Identity Governance and Lifecycle has added .zip file support 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 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 Changes in Release 7.0.2 Patch 2

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
ACM-67287	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.
SF-864475 ACM-69179	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

Issue	Description
	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. **Important:** 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" under Install a Patch.
SF-919973 ACM-72616	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.
SF-862539 ACM-70218	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.
SF-835743 SF-915044 ACM-66520	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.

Fixed Issues in 7.0.2 Patch 2

The following issues were fixed in 7.0.2 Patch 2.

Access Certification

Issue	Description
SF-803269 SF-927964 SF-979348	Specifying date-type attributes for user review criteria resulted in the following error: ORA-01840: input value not long enough for date format.

Issue	Description
ACM-63517 ACM-75730	
SF-942083 ACM-73900	Reviewers were unable to complete sign offs and received the following error message: "Failed to save the review components."
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.

Access Requests

Issue	Description
SF-959975 ACM-74600	The Fulfillment Handler was using the XML configuration instead of the internal configuration.
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.

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.

Change Requests and Workflows

Issue	Description
SF-866742	When creating a workflow for custom tasks, using the automatically

Issue	Description
ACM-69358	populated Reference Name resulted in 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 ACM-63718	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 Fulfilment Node, or generate an ORA-02291 integrity constraint error.
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-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	The workflow job history did not filter out jobs that were being deleted by the purge process, causing an ORA-01722 invalid number error.

Issue	Description
ACM-74461	
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.
SF-967811 SF-975776 SF-970135 ACM-76117 ACM-75206	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-988230 ACM-76091	The REST Web Service node could not use user data to process a response variable.
SF-996178 ACM-76578	The workflow engine was not accessible because of an invalid license.

Collector

Issue	Description
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.
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.

Connector

Issue	Description
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-877139 ACM-70139	Attribute values edited to be blank did not carry over to the connector in attribute synchronization.
SF-882233 ACM-71264	When a chain of certificates was involved in the handshake, the SOAP connector failed over 2-way SSL.

Dashboard

Issue	Description
SF-961911 ACM-74697	When the custom attribute ForcePageCleanup was used, "Request could not be handled" errors appeared when switching pages in the UI.
SF-871409 SF-905933 SF-921603 SF-927362 SF-953819 ACM-70140	The My Requests dashboard displayed incorrect values for All Requests, Pending, and Completed.

Data Collection Processing and Management

Issue	Description
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

Issue	Description
	unsuccessful run.
SF-919973 ACM-72616	The Accounts data table for an ADC incorrectly displayed the Last Collected Date after a successful run.
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-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.

Database Management/Performance

Issue	Description
SF-970037 SF-983047 SF-982768 ACM-75178	In some WebSphere environments, the WebSphere server did not deploy an RSA Identity Governance and Lifecycle application web service because it could not generate the WSDL file.
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.

Issue	Description
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.

Data Governance

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

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.

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	After a workflow update using the Workflow Editor, activity nodes in the workflow could not send email.

Issue	Description
ACM-74072	
SF-834136 ACM-69395	Email nodes in a request workflow, which were not processed within an approval workflow, sent messages with blank role names.
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.

Installer

Issue	Description
SF-888171 ACM-75828	ITIM Agent 7.0.1 did not start after installation due to a Java class error.
SF-817368 ACM-64887	Removed dependency on /tmp/aveksa/staging when running the generateLoginKey.sh tool.

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.

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	During migration, the file ACM-60520.sql was running for several hours.

Issue	Description
ACM-75848	
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.

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.

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.

Request Forms

Issue	Description
SF-843527 ACM-67287	Fields could not be added to a request form using a web service with basic authentication.

Role Management

Issue	Description
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.

Issue	Description
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

Rules

Issue	Description
SF-928144 ACM-72795	Implicit Account Removal was not working as expected.

Security

Issue	Description
SF-924000 ACM-72276	Parameters containing URLs needed additional cross-site scripting filtering mechanisms applied.

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.
ACM-75407	OpenJDK was updated to version 141 for security fixes.

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	SOAP requests sent to the ServiceNow Cloud through the SOAP web service node using proxy authentication were failing.

Issue	Description
ACM-74334	

Known Issues in Release 7.0.2 Patch 2

The following table lists the known issues for this release.

Tracking ID	Description

SF-912500 SF-960383 ACM-71838	On a Red Hat Enterprise Linux appliance, when you update or patch RSA Identity Governance and Lifecycle after upgrading OpenJDK, the following error may occur if Red Hat Enterprise Linux is missing the GConf2 package:
	
	`Caught: java.lang.UnsatisfiedLinkError: /usr/lib/jvm/java-1.7.0-openjdk-1.7.0.0.x86_ 64/jre/lib/amd64/libnet.so:`
	
	`libgconf-2.so.4: cannot open shared object file: No such file or directory java.lang.UnsatisfiedLinkError:`
	
	`/usr/lib/jvm/java-1.7.0-openjdk-1.7.0.0.x86_ 64/jre/lib/amd64/libnet.so: libgconf-2.so.4: cannot open shared object file:`
	
	`No such file or directory at CustomizeACM.run (CustomizeACM.groovy:19) An error occured in the customizeACM command : error code 1`
	
	`Step failed! See /home/oracle/Aveksa_7.0.1_ P02/logs/7.0.1_P02_2017-01-26-1337.log for more information.`
	
	Workaround: Manually install the GConf2 package using either Yum or RPM.
	
	Use the following command to install using Yum:
	`yum -y install <package file name>`
	
	Use the following command to install using RPM:
	`rpm -ivh <package file name>`

ACM-77527	A null pointer exception occurs if the user list for a change request is modified with a pending account, and the pending account is modified during change request creation.

Release 7.0.2 Patch 1

Information about the 7.0.2 Patch 1 release is included in the following sections:

- What's New in Release 7.0.2 Patch 1

- Fixed Issues in 7.0.2 Patch 1

What's New in Release 7.0.2 Patch 1

Feature	What's New
Database Management	Database statistics now exclude externally defined tables.
Role Management	Added support for large exports and imports of roles. Exported roles are provided in a zip file.
Workflow	Upgraded to WorkPoint 4.40 Patch 9.

Fixed Issues in 7.0.2 Patch 1

The following issues were fixed in 7.0.2 Patch 1.

Access Requests

Issue	Description
SF-909706 ACM-72131	On the By Entitlement tab of the My Activities page, an account's custom attributes were not populated.
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 ACM-73931	Revocation change requests did not display work items.
SF-823162 ACM-68232	The CSV file exported from Requests > Activities was corrupted.

Account Management

Issue	Description
SF-894535 SF-941753 ACM-71731	Accounts that were mapped manually from an import file before upgrading could not be unmapped in bulk.
SF-894540 ACM-71583	After deleting account mappings, entitlements associated with the mapped accounts were still displayed under the User Access tab.

Authentication

Issue	Description
SF-873800 ACM-69594	When users updated the answers to their challenge questions, saving the new values took an unusually long time.

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 is incorrectly limited.
SF-921304 ACM-72550	In the Workflow Editor, users cannot save changes to a workflow if the only change is to the Evaluated to True checkbox for a transition with the type Decision.
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-842253 ACM-67139	Tooltip messages on a rejected change request incorrectly indicated that there was an error.
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.

Issue	Description
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-920455 SF-910312 ACM-73174	When "Wait for Result" was selected, workflows were stuck in the Provisioning Command phase.

Collector

Issue	Description
SF-903111 ACM-71836	Lotus Notes collections failed when attempting to use SSL communication.
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.

Data Collection Processing and Management

Issue	Description
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-907379 ACM-71714	After enabling the Complete Manual Activity Before Collection feature, duplicate user entitlements appeared when the collector collected the added entitlements.
SF-903491 ACM-71396	Active Directory collections are failing during preprocessing, with date attribute well into the future.
SF-854003 ACM-70365	When unifying multiple IDCs, some attributes are not populated.
SF-829704	When an Active Directory account collection contained an attribute with a date value in an unsupported format, the entire collection failed.

Issue	Description
ACM-66345	
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-948261 SF-959587 ACM-73932	Identity collector can fail when USER_ID is used in a Unification Join.
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.

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.

Email

Issue	Description
SF-865404 ACM-69677	Emails containing non-ASCII (UTF) character encoding were not sent properly.

Installer

Issue	Description
SF-832386 ACM-70244	Installer and uninstaller removed Aveksa_System.cfg, which rendered the staging folder unusable for reinstallation.
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.

Password Management

Issue	Description
SF-873800 ACM-74080	Parameters containing URLs needed a cross-site scripting filtering mechanism.

Request Forms

Issue	Description
SF-918967 ACM-72683	Change request from could not be submitted if it contained required hidden tables.
SF-887157 ACM-70735	Newly created Provisioning forms did not have user variables available in the list of form fields.

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-792647 SF-836164 ACM-65704	Role status remains in Applied or Applied New State, even after change request is complete.

Rules

Issue	Description
SF-916158 ACM-72138	Rule processing failed when a rule name contains a colon.
SF-894858 ACM-71265	The Termination rule did not submit change requests to disable accounts for deleted users.

Security

Issue	Description
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-923995 ACM-72274	Multiple passes were required to fully remove disallowed HTML markup.
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.

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.

Release 7.0.2

Information about the 7.0.2 release is included in the following sections:

- [What's New in Release 7.0.2](#)

- [Deprecated Items in 7.0.2](#)

- [Fixed Issues in 7.0.2](#)

- [Known Issues and Limitations](#)

What's New in Release 7.0.2

Feature	What's New
Access Certification	The following changes have been made to Access Certification: • You can now display alternate reviewers for a particular reviewer as follows: 　• In the Review Wizard, you can add an **Alternate Reviewers** column to the **By Reviewer** tab. 　• In the Coverage File table, you can add an **Alternate Reviewers** column. • The Generate Change Request configuration option is fully supported for the Data Resource Access and Data Resource Ownership review types.
Access Request Forms	The following improvements were made to Access Request Forms: • To improve the security of request forms, the Create New Form, General Properties now includes an "Availability" filter. This filter sets who can use the form to create a request. The Availability setting was previously available on the request button used when processing a form. To run any type of form, the user must have one of the following types of access: 　• Included by the Availability setting 　• System administrator 　• Access Request Administrator entitlement • Added the ability to specify a request workflow to use when processing a request form.

Feature	What's New
	• Improved user interface for debugging a request form.
Access Requests	The following changes have been made to Access Requests: • The "Terminate User" option for the createChangeRequest command allows any user who has access to terminate a user through a web services call. See the command's description in Admin > Web Services for more information. • The UserID is included in the Manual Task Approval: User Changes section. • Accounts in web services can now be locked, unlocked, enabled, or disabled using the Operation element. • Naming policies can now be used when creating account templates. For more information, see the Help topic "Associate a Naming Policy with an Account Template." • You can now map and unmap users from accounts in the createChangeRequest web service. • From the createChangeRequest web service, you can now create a request to add a user to a group.
AFX Server	The following changes have been made in the AFX Server: • Improved logging of an RSA Identity Governance and Lifecycle response when it cannot be parsed (not in expected XML format). • AFX fulfillment requests that are stuck in the sent state for a configurable period of time are automatically resent.
AFX	The primary communication poll from AFX has been optimized for better performance. This reduces the chance of a timeout occurring while AFX is waiting for a response from RSA Identity Governance and Lifecycle.
Attributes	The following improvements have been made to Attributes: • You can create a custom value list for attributes of the integer data type that you create. • The General and the Value tabs have been removed. All configuration options are available from a single window. • When working with the "application" object in custom attributes

Feature	What's New
	(Admin > Attributes > Custom List), a third option, Name, allows for use of a "friendly" name, in addition to the Raw name.
	• You can designate user and custom attributes as public, so that the attribute appears in information pop-ups for users without explicit permissions for the object. By default, these attributes are set to private.
Audit Events	The following updates have been made to Audit Events:
	• An audit event is now logged for start up and shutdown of the application.
	• Audit events for login now include the authentication source.
Business Task Delegation / Out-of-Office Feature	Users or managers can set a user's status to out-of-office and select a delegate to act on their behalf. During the out of office period the delegate will see any approvals, activities, or reviews that would have normally been assigned to the user that is currently out of office. For more information, see the Help topic "Setting Out-of-Office Status and Task Delegation for Users."
Collectors	The following changes have been made to collectors:
	• The Lotus Notes Entitlement Data Collector has been upgraded to:
	• Collect all application file names
	• Collect Application title
	• Collect Potential Entitlements
	• Collect Actual Entitlements
	• The Lotus Notes entitlement collector supports collection of a replica ID that is mapped to a custom attribute. This allows you to collect all the versions of applications from different Lotus Note databases.
Connector Templates	Improved overall performance (rendering, searching, sorting) of the AFX > Connector Templates page.
Connectors	The following updates have been made to connectors:
	• When selecting an AFX Connector binding, the connectors are

Feature	What's New
	now sorted by group, and within each group, the connectors are sorted alphabetically.
	• Improved the performance of the Create/Edit Connector page by loading only the properties needed to render the page.
	• The default timeout value for an SSH connector has been increased to 60 seconds.
	• Audit log now includes events for creating, modifying, and deleting a connector.
Database Performance	Created an index for the WP_WORK_ITEM table to help organize the Dashboard queries. The columns are displayed in the index in the following order: • name • work_state_id • app_ref
Database Management	Database statistics now exclude externally defined tables.
Email	The following JavaMail email configuration settings are included under Admin > Email > Settings: • Mail connection timeout: The socket connection timeout value in seconds. The default value is 180 seconds. • Mail timeout: The socket input/output timeout value in seconds. The default value is 180 seconds. • Mail writer timeout: The socket write timeout value in seconds. The default value is 180 seconds.
Lieberman Enterprise Random Password Manager (ERPM) Integration	RSA Identity Governance and Lifecycle supports interoperability with Lieberman Enterprise Random Password Manager™ (ERPM) version 5.5.2 for data collection and provisioning. The combined solution enables organizations to gain a unified, policy-driven identity and access governance across all users - including the organization's most powerful identities – privileged users. RSA Identity Governance and Lifecycle provides an application wizard to simplify the process of creating Lieberman ERPM Collectors and Connectors. For more information, see the *RSA Identity Governance and*

Feature	What's New
	Lifecycle Lieberman Enterprise Random Password Manager (ERPM) Application Guide.
Password Vault Feature	You can configure RSA Identity Governance and Lifecycle to use a third-party password vault to manage the endpoint credentials for Active Directory, Oracle, DB2, and SQL Server connectors. Using a third-party password vault: • Allows you to manage and maintain endpoint credentials in a single, central location. • Eliminates the need for connector administrators to know the credentials of the endpoints that they manage. RSA Identity Governance and Lifecycle currently supports the CyberArk password vault. For more information, see the Help topic "Managing Connector Endpoint Credentials using a Third-Party Password Vault."

Platform	The following platform improvements have been made:
	
	• Upgraded openJDK from version 75 to 111 to provide the latest patches and security vulnerability fixes.
	
	• The installation script performs checks for the following installation requirements:
	
	    • Memory
	
	    • Operating system packages
	
	    • Network settings
	
	    • User and group settings
	
	    • System configurations
	
	The installation script displays information about the checks, and it indicates if a requirement is not met. After you resolve the requirement, you can run the script again.

Pre-upgrade Report	The Installer now performs pre-requisite checks to determine whether an installation/upgrade host is set up correctly for installation.
Rules	The following improvements have been made to Rules: • Improved change request generation action performance.

Feature	What's New
	• Added a new processRule web service.
Security	Changed dynamic SQL to use bind parameters in miscellaneous packages to prevent SQL injection and enhance performance.
Server Core	
Simplified Approvals	The approval process is now streamlined as new approval workflows now suppress indirect entitlements by default. Approvers see only the direct access entitlements needed for an approval. You can change this setting to display indirect entitlements using the properties page in the approval workflow node.

User Interface	The following improvements have been made to the user interface:
	
	• The What's New dashboard is now available to any user who is assigned the System Administrator privilege.
	
	• The following tooltips are added to the images:
	
	   • Info icon - Click for additional details
	
	   • Keys on login screen - Please enter your login credentials
	
	   • Icons on the Home page - Match the gray text already shown beside the image.
	
	• Product name is displayed as RSA Identity Governance and Lifecycle throughout the user interface.
	
	• The RSA Identity Governance and Lifecycle login screen has been updated.
	
	• Character limits for custom attributes are now displayed in the database ID dropdown.

Web Service	The following updates have been made to Web Services: • The processRule web service command either accepts the name of an active rule in the system or processes all of the active rules. This command can only be run by users that have the Rule:Admin privilege. The command returns the status of the other rules. • The updateReviewItems command lets you update one or more items in a user access review that is in an actionable state. See the command's description in Admin > Web Services for more

Feature	What's New
	information.
	• Added a new capability to the createChangeRequests web service to allow mapping of users to accounts. This capability provides a way to update an account mapping within a workflow. See the command's description in Admin > Web Services for instructions on how to use the "Map user to account" capability.
	• Support for Single Sign-On (SSO) to authenticate users of Web Services.
Workflow	The following updates have been made to workflows:
	• Under Admin > Workflow, the new Monitoring tab displays real-time information about the workflow queue status.
	• Upgraded to WorkPoint 4.40 Patch 7.
	• Improved status displayed for a change request to show why a request was completed by the system and any associated error state.
	• An email address is now supported as a workflow variable's value for selecting a resource.
	• Improved appearance of nodes in Workflow Editor.
	• The default view on Admin > Workflow > Jobs now displays Active jobs instead of all jobs.

Deprecated Items in 7.0.2

Feature	What's New
Database	The V_CHANGE_REQUEST_DETAILS database view has been deprecated. It no longer serves the purpose it was originally designed for, and input/output operations with the table degraded system performance.
Patch Documentation	Patch_README.txt has been removed and the content is now included with the Installing a Patch documentation.
User Interface	Changes to Admin > User Interface include: • For new installations, the RSA style user interface option is the only style available.

Feature	What's New
	• For upgrade installations, the preferred non-RSA style from the legacy version is retained as a style option. The only other available option is the RSA style
Workflow	The following deprecations were made to the Workflow Editor: • The legacy Workflow Editor applet has been fully deprecated as of this release. • The option to reset the job was removed from the job menu in the Workflow Editor.

Fixed Issues in 7.0.2

The following issues were fixed in v7.0.2.

Access Certification

Issue	Description
SF-765844 ACM-60264	Quick filtering on the User Detail's Requests tab consumes an inordinate amount of database resources.
SF-775551 ACM-61215	Submission variable is not appearing on all Change Requests, when the Change Request uses a custom form with grouping by user and multiple users are submitted. This issue has been fixed so the variable now appears on the Change Request for each user.
SF-615728 ACM-52615	When the account is switched to Maintain state, the account sub-components become actionable and when the account is Revoke state, the account sub-components become locked.
SF-627462 ACM-52588	A change request generated for a user who has an account revoked in an account access and ownership review does not appear in the user's Requests tab.
SF-859909 ACM-68441	A "Comments have not been added for N revoke items. Please provide comments for these items." message appears after sign-off in an account access and ownership review even though comments have been added to signed off review items.
SF-810120 ACM-64976	When running a User Access review with the Include sub-groups option checked under Content, no users who are members of the selected group

Issue	Description
	are included in the review.
SF-827134 ACM-65820	Count reported in review status message does not match items selected in the review.
SF-875454 ACM-69612	A review generation is stuck on a certain step due to performance issues caused by the STG table.
SF-791436 ACM-62724	In a Group Review result, previously set table defaults do not appear.
SF-756275 ACM-59397	When multiple review escalations are scheduled for a single review, the review is incorrectly reassigned.
SF-818814 ACM-64986	Some review templates use an incorrect variable for delegation comments.
SF-820993 ACM-65054	In Group Reviews, when signing off a deleted group item, a null pointer exception occurs.
SF-889059 SF-911366	A review that was unable to complete caused an error during restart that prevented the user interface from loading.
SF-845777 ACM-67417	Exceptional temporary access to entitlements granted in a user access review stayed in the Maintain state after the expiration date.
SF-823074 ACM-65494	A user access review does not allow reassignments after changes to the review have been saved.
SF-823353 ACM-65307	Review items that are maintained with an expiration date are designated as signed off even though sign off is not specified for those review items.
SF-816567 SF-834552 ACM-64937	A review took a considerable longer amount of time to complete in a production environment after an upgrade.
SF-805551 ACM-63789	A review "Due by" field displays "(null days left)".

Issue	Description
SF-792006 ACM-63562	In an account access and ownership review, the group by Account User filter does not work.
SF-799972 ACM-63350	Account review generation fails when using Turkish (double-byte) characters in the display name.
SF-784527 ACM-62533	Selecting the 'Created On' attribute multiple times in the Table Options, duplicates the columns in the Change Preview tab.
SF-785022 ACM-62505	User review shows the direct membership of nested roles.
SF-780558 ACM-61585	On the Account Selection page, LAST_LOGIN_DATE attribute is not displayed in the Filter accounts section.
SF-771497 ACM-61396	User access review items are unassigned after uploading the Coverage file that specified reviewers.
SF-771705 ACM-61364	When the first step does not get generated, the second step review generation fails with unique constraint error.
SF-777907 ACM-61295	When filtering business sources in the Review Definition, using an SQL statement with new lines in query leads to an ORA error during review generation on Weblogic.
SF-772393 ACM-61086	An account review is completed but the Completed Status bar indicates that it is not completed.
SF-750619 ACM-60722	When the monitor tries to access a review using the hyperlink created from the variable review_rvw_url, an insufficient privilege error appears.
SF-757199 ACM-60655	When the option "Allow monitors to update their review metrics" is unchecked, it cannot be saved.
SF-755960 ACM-59438	In the Reviewer Reassignment escalation workflow, the Outlook Email Address is reassigned to the wrong user.
SF-748387 ACM-58768	When creating a User Access Review definition, in order to select users to be reviewed through "Include users with the following attributes:", the user must add the e-mail address through the Advanced page, not the Simple page.

Issue	Description
SF-748712 ACM-58549	The reported reviewer is wrong for the reviews that use the alternate reviewer coverage file.
SF-697502 ACM-55009	When the reviewer reassigned a review item to other reviewers without giving them the sign-off privileges to delegate, the review item is not removed from the former reviewer's list, even if "Remove selected items from my review" function is selected.
SF-696093 ACM-54926	Group entitlements are unassigned in the user access review.
SF-676846 ACM-54817	The 'Overall Status' in the Review Result refreshes automatically to update the displayed time and date even after the completion of the review.
SF-664646 ACM-53395	"On Hold" reviews appear as pending actions on reviewer's homepage rather than just the "Active" reviews.
SF-627462 ACM-52588	A change request generated for a user who has an account revoked in an account access and ownership review does not appear in the user's Requests tab.
SF-20142 ACM-46894	Groups which are direct or indirect entitlement to the Role are not filtered out as "not in Role with" option in Group Review.
SF-19497 ACM-45742	A user access review result incorrectly displays decimal points in job code IDs when the results are grouped by job code.

Access Requests

Issue	Description
ACM-65578	When a form with the Display option enabled is run, the User Account Table does not load accounts and displays a count of 0.
SF-825567 ACM-66659	Only the prefix for a change request is displayed in the Requests window when the workflow that initiates the request for a Provisioning-Termination rule violation is configured with that prefix.
SF-768662 ACM-62557	Not all information questions provided in a request form are displayed to a user who is requesting access.
SF-769981 SF- 780942	Accounts created from an account template are not removed from the user interface when the request item is rejected and canceled.

Issue	Description
ACM-60837	
SF-841932 ACM-67259	The selected user in a request form is lost if the user has multiple first or last names.
SF-802569 ACM-63890	When activities are filtered by the "By Assignee" tab, activities are duplicated as many times as the number of tasks that are in the activity.
SF-803077 ACM-63981	The configuration of hidden fields in a request form is causing an error condition when a requestor attempts to create the request.
SF-791705 ACM-63460	A canceled change request did not show who canceled the request. The request now shows who canceled it and when.
SF-799755 ACM-63214	In a Request Form, conditions may not behave as expected due to incorrect unicode/UTF-8 handling in dependent field values that contain unicode characters.
SF-828369 ACM-66081	A role that contains users stays in the Open state after an attempt to delete it has been made.
SF-798406 ACM-63215	All requests for a particular application are auto canceling.
SF-804303 ACM-63641	A completed request is still shown in the Fulfillment Phase in Request Details screen. The fix makes sure that the request is processed and moves to the completed state.
SF-796872 ACM-62981	The Entitlement Name field is not required when creating a request form for a new group access for UNIX platform.
SF-775755 ACM-61928	Required entitlement field in Access Request form is empty, but form is still submitted.
SF-751445 ACM-60780	When the user attempts to view the Entitlement tab under Activities page, the UI generates a stack overflow error.
SF-709543 ACM-55802	When Change request initiates via Roles, the Account Changes table shows 'Error' message.
SF-700719 ACM-55535	Users lose the "Other Business/TechnicalOwner" or "Other Violation Manager" entitlements to business sources when a business source that had

Issue	Description
	these entitlements granted to users is deleted.
SF-804825 ACM-63833	Change Requests for entitlements are not created with the necessary Create Account items for those entitlements.
SF-799702 ACM-67147	Create account change items for indirect entitlements are not rejected when the related direct entitlement (role) is rejected in a change request.
SF-837963 ACM-66702	Selected user for reassignment is lost when switching between tabs
SF-822954 ACM-65328	In SOAP and REST Nodes, embedded variables are not being substituted correctly and are sent as null.
SF-869744 ACM-69209	Default value for text field is set always now, regardless of display conditions.
SF-825742 SF-768664 ACM-68221	When adding entitlements to users, some account template forms are not displayed.
SF-825742 SF-768664 ACM-68221	When adding entitlements to users, some account template forms are not displayed.
ACM-65578	When a form with the Display option enabled is run, the User Account Table does not load accounts and displays a count of 0.
SF-709543 ACM-55802	When Change request initiates via Roles, the Account Change table shows 'Error' message.

Account Management

Issue	Description
ACM-58035 SF-00736035	When attempting to add entitlements to a user with multiple accounts, the account is incorrectly displayed as Disabled = False
SF-747310 ACM-59551	Exported .CSV files are erratically missing information and incorrectly duplicating information.
SF-811933	Group membership is not displayed under **Users** > **Me** > **What Access** > **Account** > **Groups**.

Issue	Description
ACM-64492	
SF-909993 SF-907746 SF-906213 SF-915126 SF-917341 SF-929895 ACM-71772	ADCs are failing with the following error: "Unprocessed Continuation Reference".

ACM Security Model

Issue	Description
SF-825335 ACM-65610	A non-privileged user can generate a change request by changing the OID value in the change request URL.
SF-828016 ACM-65765	A non-privileged user can edit Attribute Synchronization settings.
SF-828015 ACM-65761	Non-privileged user can edit AFX connector and change the capabilities.
SF-792313 ACM-63539 ACM-63537	Authorization bypass to product features is observed.
SF-654596 ACM-52863	Removed the Workflow Admin entitlements from the Role Administrator app role. The Role Administrator role is responsible for managing roles, but was not meant to also design or modify workflows.

Admin Errors

SF-785277 SF-808843 SF-813273 SF-813716 SF-779942 SF-798641	Various errors reported when using an SQL command in a Workflow node, including "SQL command not properly ended," "Valid query in workflow node fails," and statement fails with "Invalid column index." This fix eliminates these errors with SQL commands. Quotes are no longer needed nor suggested around variable names. For backward compatibility, if the quotes are included, they are ignored. Whitespace between the opening quote and closing quote, or q-quote wrapper, are also ignored.

SF-785277	All of the following are equivalent:
SF-793594	${access_request_notes}
ACM-62821	'${access_request_notes}'
ACM-64434	q'[${access_request_notes}]'
ACM-64408	q'{${access_request_notes}}'
ACM-61859	q'(${access_request_notes})'
ACM-62731	q'<${access_request_notes}>'
	q'!${access_request_notes}!'
SF-847001 ACM-67378	Application crashes and aveksaServer.log shows "too many open files" error.

AFX Server

Issue	Description
SF-850602 ACM-67569	For the Office365 Connector, the default value of encrypted parameters for capabilities are shown in clear text in the user interface.
SF-749898 ACM-58642	AFX download server delivers a zero size file when there is not enough space user /tmp. This error was indicated in the log file, and is now also shown in the user interface.
SF-762063 ACM-59782	Extra files AFXPlugIntemp_connector_migrationafx-connector appeared in the WEB-INF/plugins directory.
SF-781577 ACM-62459	In a cluster setup, a connector test request sent from a non-SON node results in a request timeout error. This issue would occur on all three cluster types (WildFly, WebSphere, and WebLogic).
SF-806147 SF-806198 ACM-63935	AFX requests that fail to fulfill at the target system get stuck and do not create manual activities (in AFX fulfillment workflows) or move to the next workflow node (when provisioning command nodes). This issue was fixed by accounting properly for Unicode characters.
SF-625568 SF-620646 SF-668423 SF-680413	False AFX failures occur when adding or removing user accounts from groups in Active Directory.

Issue	Description
ACM-52843 ACM-51871	
SF-760264 ACM-60527	Test Connection for Soap Connector to Lync AFX fail.

AFX-Workbench

Issue	Description
SF-711897 ACM-55731	AFX connectors do not install when moving from development to test box in WebSphere environment.

Appliance Updater

Issue	Description
SF-838853 ACM-66832	The *Appliance Updater Guide* did not cite a disk space requirement for an update.

Application Wizards

Issue	Description
SF-710124 ACM-55896	Problems occurred with a ServiceNow collector connecting to ServiceNow FUJI version.
SF-815734 ACM-66015	A Request.Loader error occurs when attempting to "Next" to the last page in a collector definition wizard.

Authentication

Issue	Description
SF-619882 ACM-51714	BindPassword of authentication source is now obscured properly.
SF-902476 ACM-71363	When the optional token header is not specified, the error "SSO token header key class is not set" is incorrectly shown.

Change Requests and Workflows

Issue	Description
SF-847442 ACM-67439	AFX not processing requests due to active workflows with no change request entries.
SF -802638 SF-797279 SF-789403 ACM-64929	Requests will not pass the verification stage even though watches are completed and changes are collected, which prevents Workflows from progressing.
SF-764114 ACM-63918	A workflow definition specifies that a change request approval should be assigned to the rule owner, but it is assigned to AveksaAdmin instead.
SF-763404 ACM-59907	A change request to commit changes to a role takes an inordinate amount of time to complete.
SF-762350 ACM-59820	The workflow gets an error at the Workflow Path and stops.
SF-797168 ACM-64217	The Overall Status bar on Request status does not show completed (100 % green) when the change request is forced to complete. This issue was fixed so that the Mark Verified node gets the Request Form item.
SF-764114 ACM-67485	For a change request with multiple rule violations and different owners, approval goes to only one rule owner.
SF-838478 ACM-66673	An "IndexOutOfBoundsException" error occurs when clicking on the "Form" tab in any activity node having less than two outbound request-button transitions.
SF-792922 ACM-63524	Accounts were enabled multiple times.
SF-747182 ACM-58834	When requesting access, clicking the submit request button, and then clicking Cancel results, accounts with a placeholder value are created in the database and shown under the user.
SF-844480 SF-843836 ACM-67253	Unable to submit change requests or complete existing workflows.
SF-813050	In a Default Approval Workflow, incoming and outgoing transitions cannot

Issue	Description
ACM-65950	have the same name, or same synonyms.
SF-813273 ACM-64373	Performance issue observed closing watches in requests due to large-sized requests and inefficient processing of JMS events.
SF-814672 ACM-64795	An approval rejection for one user causes rejection of account changes for other users.
SF-812262 ACM-64497	In a workflow, an Approval node is disconnected from the Approvals phase when using Group By Role Owner.
SF-791651 ACM-63736	A workflow produced an "Ora-01873" error.
SF-803677 ACM-63495	Workflow stays in the Created state until it is manually evaluated.
SF-21843 ACM-48378	Workflow SQL parser is unaware of quote delimiters when using form variables.
SF-746921 ACM-58879	If the change request is stuck with no created workflow, closing the change request keeps the Roles in the applied state rather than revert them.
SF-705452 SF-709315 ACM-55366	Error occurs during request fulfillment: "ORA-01722: invalid number."
SF-795604 ACM-63164	Form approval node produces an error.
SF-791879 ACM-62654	An error message appears when the Decision node connects the Fulfillment Phase Node and Form Fulfillment Node. The fix now allows a Decision node between the Fulfillment Phase Node and Form Fulfillment Node.
SF-776459 ACM-62468	In custom tasks, "Can Run Manually" and "Administrator can run manually" filter conditions were not working. Now, "Can Run Manually" lets the user listed in the filter run the task with the 'Run' button enabled. "Administrator can run manually" now considers the user as an administrator if he or she has an App Role as a Access Request Admin.
SF-620305	Terminating a user through Default Terminate Button, Default Terminate

Issue	Description
ACM-52017	Form, or default workflow duplicates change requests.
SF-745588 ACM-60984	The user using the REST Web Services Node is unable to set "Content-Type", which instead defaults to "text/plain".
SF-775143 ACM-60989	When the big role changes are requested, it takes a long time to create the change request.
SF-820125 ACM-64971	An escalation email created from each job approval contains a list of all users affected by the main Change Request, instead of just the affected user.
SF-815249 SF-787876 SF-808059 SF-823486 SF-812840 SF-835037 SF-867034 SF-851571 ACM-65010	When a change request that includes creating an account is created by a Role rule, the request creates a pending account with the wrong account name.
SF-853427 SF-849624 ACM-67871	Authentication fails if the authentication source uses an Account Data Collector and the AccountSearchAttribute is different than the distinguishedName (used as the Account Name).
SF-00796817 ACM-63595	When a request is generated via form without any other entitlements, the email templates do not display the value in the optional comments field during a Form Approval/Fulfillment.
SF-858765 ACM-68800	The Reject button is missing in a change request Approval form.
ACM-67691	When setting a condition in a transition, the operand values are not available
SF-799005 ACM-63385	A change request is created and completed without approval or fulfillment when the business source has "Entitlements require accounts," the user has multiple accounts in that business source, and the workflow properties are set to the attribute "group jobs by any user."
SF-00861544 ACM-68868	In a workflow transition line, entering anything past the character limit of 64 generates an error.

Issue	Description
ACM-69623 SF-876459	After saving information in the settings of a Java Node, the fields "Java Class" and "Method" are empty upon reopening.
ACM-69809	When attempting to set a transition as Conditional, it will reset to Unconditional unless the user sets and saves it a second time.
SF-872423 ACM-69448	Updating one Decision Node to use a condition of "Workflow Variables" will auto-populate any other Decision Node(s) to use the same condition form.
SF-810396 ACM-63051	Even though an account is present in two different applications, the workflow only creates one task.
SF-880897 ACM-70091	Changes and configurations in the new workflow nodes are not saved properly.
SF-746543 ACM-63437	During account creation, when AFX reports a failure due to a duplicate user, the associated change request reports a success.
SF-893870 ACM-70786	If an account has been deleted before a Change Request item has been fulfilled, upon completion of fulfillment node a null pointer exception occurs.
SF-814796 SF-840524 SF-817772 SF-804825 ACM-67872	When a change request is not successfully submitted, pending accounts remain in the system until manually cleaned up.
SF-928182 ACM-73104	The number of escalations in a workflow is incorrectly limited.
SF-921304 ACM-72337	When configuring a decision node to check whether a workflow variable exists, the Right Operand field is incorrectly required.
SF-921304 ACM-72550	In the Workflow Editor, users cannot save changes to a workflow if the only change is to the Evaluated to True checkbox for a transition with the type Decision.
SF-910461 ACM-71747	In the Workflow Editor, when using a user data variable that has multiple values, these values are being returned as a space separated list, which causes an error.

Issue	Description
SF-742983 ACM-57810	When a request contains approvals for more than one entitlement and the entitlements have different Data Owners, the escalation workflow assigned the approval to the incorrect Data Owner.

Collector

Issue	Description
SF-764480 ACM-60052	Customer cannot use the word 'Replace' as part of the SQL query in the Entitlement collector.
SF-764483 ACM-60476	Identity collections fails. The following error is observed in aveksaServer.log: "ORA-01400: cannot insert NULL."
SF-719853 ACM-56512	The system updates the database with partial read results after an LDAP collection when a search operation is abandoned or terminated.
SF-759424 ACM-59853	Workday Identity Collector fails with an error "Failed to add WS-Security header to request"
SF-792326 ACM-65487	LDAP Account data collection process stuck.
SF-754154 SF-771853 ACM-59329	Cannot collect from a cloud-based Workday application without the ability to define the web proxy.
SF-825862 ACM-66486	When testing Google Apps collector, a "null pointer exception" error is returned.
SF-795519 SF-822221 ACM-64496	Office 365 Account Data Collector (ADC) does not collect accounts properly when more than 500 accounts.
SF-795752 ACM-63469	Lotus Notes Account Collector does not collect Group data.
SF-820416 ACM-66457	LDAP Collector will not bind over TLS 1.1/1.2.
SF-793943	The Active Directory identity data collector is not able to collect users through encrypted and non-encrypted LDAP servers.

Issue	Description
ACM-62896	
ACM-61775	The Lotus Notes entitlement collector does not support collection of a replica IDs. See What's New in Release 7.0.2 for more information.
ACM-63917	Use of the "Test" button when creating or changing a collector configuration causes the system to become unresponsive.
SF-770400 SF-756694 ACM-60732	MAL: The connection to remote agents timeout, interrupting the collection process.
SF-783309 SF-766351 ACM-61786	The field "Security Token" appeared mandatory in the new SalesForce Data Collector configurations.
SF-755785 ACM-61422	In the Applications > Account tab, The table column does not display Custom Attribute Integer 4 (CAI4) after the data was collected.
SF-697411 ACM-55178	The account collector search scope only returns the first group and member of the group.
SF-792812 ACM-62643	The Entitlement Data Collector does not work with a custom database driver after the upgrade.
SF-730437 SF-808076 ACM-57967	After updating MySQL driver to v5.6, the Active Directory Collector (ADC) test fails with a SQL syntax error.
SF-758164 ACM-62486	StealthAUDIT did not collect data from IP addresses ending with the .255 octet.
SF-856748 ACM-68577	When a Change Request is created for a directory, "Other Type" owners are ignored for approval/fulfillment.
SF-855812 ACM-68176	Disabled accounts collected using the Lotus Notes collector are incorrectly displayed as active.
SF-792812 ACM-62643	The Entitlement Data Collector does not work with a custom database driver after the upgrade.

Issue	Description
SF-775274 ACM-64003	A collection with incorrect data and a large data set did not result in an expected admin error.
ACM-63917	In some circumstances, the Test functionality for newly created or modified collectors causes the application to become unresponsive.

Connector

Issue	Description
SF-828448 ACM-65814	Connector password mapping strips password containing certain special characters.
SF-829366 ACM-65491	Lotus Notes Collector: Failed to execute with error as ID file directory is required.
SF-779202 SF-773511 ACM-62921	When using SSL with the generic SOAP Web Services Connector, AFX ignores any certificates in the default truststore or any keystore paths specified in the UI connector configurations.
SF-758811 ACM-60041	SOAP connector fails with a NullPointerException.
SF-650965 ACM-53908	When configuring the REST Web Services Connector, the Command Code Path input field cuts off all of the content after "&".
SF-835268 ACM-66722	When creating an account using the Active Directory connector, the connector does not accept more than 26 parameters.
SF-810184 SF-820915 SF-842422 ACM-66623	Creating an account with an initial password (using the Active Directory connector) fails because password is not accepted.
SF-861720 SF-871676 SF-877268 ACM-68574	When configuring an account collector to collect groups to sub-groups membership, the resolution fails and the sub groups are collected with type "Account" under the "Member Type" field.
SF-875669 ACM-70229	Unable to execute or call Stored Procedure using Generic DB - SQL Server 2000 connector.

Dashboard

SF-773609 ACM-60921	RSA Identity Governance and Lifecycle is not displaying dashboards according to the display sequence.
SF-741584 SF-795450 ACM-62634	The Dashboard shows the default review tabular report instead of a tabular report specific to the review you clicked on.
SF-778398 ACM-61346	User experiences long response times when using the Dashboard.

Data Collection Processing and Management

Issue	Description
SF-831525 ACM-66720	The Monitoring page loads data slowly.
SF-857043 SF-845341 ACM-68196	Entitlements granted by manually mapped accounts do not appear under a user's Access tab after an upgrade from 6.5.1.
SF-757246 SF-757712 ACM-59587	Users with null on unification join attribute are rejected. The following unification error is observed: "EC[102] Context[RunID=60245, IDC (ID=21)] Message[Identity Data Validation: One or more attributes user in Join Condition has duplicate values.]"
SF-767428 ACM-60387	The A_AVR_ACCOUNT_ENTITLEMENTS view is deleted after running a collector a second time.
SF-771363 ACM-60734	Entitlements cannot be mapped to users if a multi-app entitlement collector is deleted.
SF-767681 ACM-60520	Unification and Aveksa ADC processing never completes after applying 7.0 P01. Both tasks are required to be canceled using the Kill Task option in the Run Details page under Admin > Monitoring.
SF-769891 ACM-60586	The "Data is case sensitive" setting for an account collector is ignored, resulting in 40,000 orphaned accounts.
SF-763198 ACM-60872	Manual account mappings are not cleared after collected data indicates they should be cleared.

Issue	Description
SF-596695 SF-743574 ACM-50656	WebSphere logs the following message "There are currently 100 open JMS Producers for the Session." This has been fixed so that the application closes producers that are not required.
SF-829517 ACM-66144	Identity collection from an Active Directory source fails during the identity load step with this error: "ORA-01489: result of string concatenation is too long."
SF-824159 ACM-66572	Rendering a view of business descriptions is slow after an upgrade to 7.0 patch 3 from 7.0 patch 2.
SF-773829 SF-818058 ACM-64376	Identity collection from an LDAP source fails with multiple Oracle errors.
SF-740736 ACM-59192	When upgrading from 6.9.1 P06 to P07, entitlement data collectors are unable to complete the collection process.
SF-806113 ACM-64113	SQL validation failing for data collectors.
SF-789930 ACM-62400	Business description processing taking 30 minutes to process 168,000 records.
SF-816288 ACM-64737	Data collection information is not displayed under the Admin > Monitoring > Performance Summary tab.
SF-814183 ACM-64739	The following error is observed in system logs after an upgrade from v6.5.1 to v7.0: "ORA-01400: cannot insert NULL."
SF-822257 SF-823791 ACM-65165	When creating an entitlement collector, the Resource Entitlements Query does not support an SQL entitlement column and produces an error.
SF-835271 ACM-66936	Missing group memberships are not correctly updated in the database.
SF-808921 ACM-63946	Unification has been running an inordinate amount of time.
SF-806508	Indirect relationship processing is inordinately slow for collected

Issue	Description
ACM-63818	entitlement and role data after applying 7.0 P02.
SF-792371 SF-797976 SF-815955 ACM-62549	Change verification after account collection taking 14+ hours.
SF-800847 SF-807868 SF-808385 SF-812247 ACM-63717 ACM-64481	An entitlement collection fails. The following error is observed: "failing with ORA-30926: unable to get a stable set of rows in the source tables."
SF-782956 ACM-61793	An "ORA-30004: when using SYS_CONNECT_BY_PATH function, cannot have separator as part of column value" error occurred when performing a query on V_BIZROLES_MEMBERSHIPS.
SF-801859 ACM-63464	Account collection is failing in development and production environments.
SF-758073 ACM-59428	The entitlement collector fails during the database processing stage.
SF-774660 ACM-60969	Unification taking in an inordinate amount of time to complete.
SF-762463 ACM-60443	Cannot use the REPLACE keyword in collector queries.
SF-801042 ACM-63358	Account collection is taking an inordinate amount of time to complete.
SF-800215 ACM-63298	Identity collector indirect relationship processing taking seven hours and deleting user relationships.
SF-793794 ACM-62780	Unification fails at step 5/10 with this error: "ORA-30926: unable to get a stable set of rows."
SF-762813 ACM-60776	The field in the Entitlement Data Collector table was not big enough to support concatenating Resource Name and Action fields.

Issue	Description
SF-758596 ACM-59675	After the customer rebuilt a collector, they could no longer submit requests for their roles.
SF-838492 ACM-66721	Entitlement collection from Active Directory fails at the "DataValidation.AppRoleCycleCheck" step.
SF-725770 ACM-56683	Concurrent user logins slow down the user interface and show the "loading data" message.
SF-845485 ACM-67600	Data unification did not complete.
SF-814121 ACM-64423	A duplicate user is created after moving the user from a collector with lower priority to another with higher priority in a data unification configuration.
SF-868656 ACM-69142	Active Directory group memberships are not updating correctly when a user moves to another organization unit.
SF-835512 SF-831117 ACM-66909	Collector REQUIRES_FULL_REFRESH values not working as expected in 6.9.1.
SF-881281 ACM-69893	The "Active and Availability" status incorrectly shows the user as active despite being terminated or deleted.
SF-883207 ACM-70129	The Identity Collector Unification runs for an extremely long time during data clean up.
SF-877679 ACM-69665	Account Data Collectors are taking much longer than expected to execute and appear to be stuck on a single step.
SF-00824995 SF-00812645 ACM-65488	When the Identity Collector is running, the order of the two tasks are incorrect: first data processing is completed, and then the data collection runs, while it should be reversed.
SF-843099 ACM-67381	The Active Directory ADC is unable to collect group memberships for accounts with DNs longer than 256 characters.

Issue	Description
SF-862232 ACM-70364	When an application and rule set have the same name, the account mapping gets rejected while resolving application references, because the name resolves to the rule set.
SF-758832 ACM-62291	When the truncate data option is selected, strings with multi-byte data are not properly parsed.
SF-854003 ACM-70365	When unifying multiple IDCs, some attributes are not populated.
SF-920141 ACM-71086	Role data collection fails with the following error: ORA-06536: IN bind variable bound to an OUT position.
SF-805942 ACM-67393	When an invalid Business Unit is updated in a collection, a user's data is not properly updated in the UI.
SF-737360 ACM-57480	The Active Directory ADC is unable to map the group owner to a user attribute that is longer than 256 characters.
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.

Data Governance

Issue	Description
SF-825171 ACM-69369	When a member is deleted from a local role and then added again, duplicate entries for that member are created in the T_AV_ ROLEMEMBERSHIPS table.

Database Management/Performance

Issue	Description
SF-824709 ACM-65504	AveksaAgent and AFX become unresponsive in a high network usage scenario.
SF-744512 ACM-57938	Review generation is very slow after the migration from version 6.8.1 P11 to 6.8.1 P21.

Issue	Description
SF-784081 ACM-64480	A performance issue is experienced with the SecurityContext.csv query.
SF-840381 ACM-67302	The system is inoperable because of a "Unable to start service ChangeRequestService" error, which is precipitated by a "ORA-01403 in UTILITIES_PKG" error.
SF-760015 SF-784081 ACM-60459 ACM-64559	Slow performance experienced with the system. In Requests> Activities, accessing "ActivityByBusinessSourceTable" results in long-running process.
SF-829784 ACM-65974	When using avdbimport to import a database backup, entering the wrong name for the backup file results in an empty database.
SF-783596 ACM-61770	Leaking CLOBs and XMLType exceeded maximum temporary space over a period of time.
SF-782388 ACM-61635	An "ORA-01000: maximum open cursors exceeded" error occurred when a report was generated.
SF-799174 ACM-63105	Slow page load observed in the Requests > Activities > By Entitlement page from a monitoring policy view.
SF-767203 ACM-63649	A requestor is experiencing delays in navigating through the change request procedure when requesting access to a role.
SF-788716 ACM-62503	During migration to 6.9.1 P7 and above, the migration script produced duplicate data in the UNDO tablespace, causing the patch installation to fail.
SF-848601 ACM-67758	A query in a workflow against V_AVR_ACCOUNT_ENTITLEMENTS is not returning results.
SF-851870 ACM-67724	A view table is missing the expiration date column, forcing users to look elsewhere for the information.
SF-867169 ACM-69593	An SQL table rendered an error when it encountered an incorrect alphabetic character instead of a numeric one.
SF-824730	A performance issue is observed with Admin > Email > Log.

Issue	Description
ACM-66406	
ACM-60600	The V_CHANGE_REQUEST_DETAILS database view has been deprecated. It no longer serves the purpose it was originally designed for, and input/output operations with the table degraded system performance.
SF-909861 ACM-71764	On startup, if the database time zone check determines that the time zone needs to be changed, it attempts and fails to change the time zone, and restarts the database.

Descriptions

Issue	Description
SF-826482 ACM-65590	The Long Description is not applied correctly for an object after a metadata file import and the description filter contains an underscore (_) character.

Documentation

Issue	Description
SF-903690 ACM-71356	Product documentation referred to an incorrect product name.
SF-799242 ACM-63126	The RSA Identity Governance and Lifecycle Connector Data Sheet for JAVA Code Base was missing instructions on obtaining the JCBC_SDK.zip file.

Email

Issue	Description
SF-815444 SF-826425 ACM-64605	Password change emails queued with no justification.
SF-713802 ACM-55974	A Long Description hyperlink does not open in a new window/tab, rather the current window is replaced by the hyperlink URL.
SF-797673 ACM-63343	After the email server goes down, RSA Identity Governance and Lifecycle does not send emails until restarted.

Installer

Issue	Description
SF-762176 ACM-60865	Patch installation fails if an "admin" account does not exist.
SF-781349 ACM-61906	The /home partition minimum error message is inaccurate.
SF-849575 ACM-68165	The common.sh scripts fails on instant client because the oracle user does not exist.
SF-849575 ACM-68191	A remote database install fails to check the database version in a software-appliance deployment scenario.
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-841751 ACM-67014	An unnecessary check for an OS generated an error when attempting to upgrade the JDK patch.
ACM-61693	Upgrading RSA Identity Governance and Lifecycle on RedHat 5.11 failed because the oracleasm RPM was removed.
SF-737562 SF-752438 ACM-58108	The installer script did not check for prerequisites for Oracle 12 before uninstalling Oracle 11.
SF-832386 ACM-70244	Installer and uninstaller removes Aveksa_System.cfg, which renders the staging folder unusable for reinstallation.
SF-733521 ACM-70207	Upgrade prerequisite check is performed after the previous version is uninstalled.
SF-860329 SF-873678 ACM-69107	The installer aborts with the error: Current swap size of "16777212 KB" is less then needed minimum value of "16777216 KB".

Localization

Issue	Description
SF-847195 SF-844392 SF-850076 ACM-67255	Files uploaded from Admin > User Interface disappear after restarting the application services in 7.0 P04.
SF-690541 ACM-54612	Request buttons are not language localized.

Local Entitlements

Issue	Description
SF-763467 ACM-60229	A user with a "Directory: Admin" entitlement is not able to edit Groups.

Metadata Import/Export

Issue	Description
SF-820237 SF-811129 ACM-65049	A directory reference ID is incorrect after an XML file export.
SF-879692 SF-880264 SF-893319 ACM-69761	Exporting collector definitions from a 7.0.1+ system and importing them into another 7.0.1+ system results in a failure with encryption errors.

Migration

Issue	Description
SF-802279 ACM-63383	Invalid characters within a XML CLOB prevents data runs after migration.
ACM-68767 SF-00865554	During upgrade, the migrate.log reports the error "single-row subquery returns more than one row" because part of the update query is looking to match against old records
SF-821693 ACM-65538	A performance issue is observed with indirect relationship processing.

Issue	Description
SF-766236 ACM-60263	Migration Error: Only one PARALLEL or NOPARALELL clause may be specified during migration.
SF-859336 SF-879000 SF-904095 ACM-68259	Many invalid objects database observed after migrating from 7.0.0 P03 to 7.0.2.
SF-821693 ACM-65205	Migration is taking an inordinate amount of time to complete. An issue with the get_duplicate_Accounts function in the Pre_migration_pkg.pkg was observed.
SF-974794 ACM-75390	Database migration to 7.0+, when applying the ACM-61839.sql patch, did not succeed due to Oracle error ORA-30926 because groups with duplicate names are no longer allowed when collected for the same application by different collectors.

Password Management

Issue	Description
SF-815454 ACM-65457	In a Password Reset form, the Preview Table in the User Account Table is not displaying accounts.
SF-751426 ACM-60715	The specified parameter for 'Maximum repeated characters' in a password policy does not save after the user changes it.

Platform

Issue	Description
SF-689578 ACM-54594	Running the modifyhostname.sh script on V6.9.1 fails with a " /usr/bin/modifyhostname.sh: line 157: ../acmcerts.sh: No such file or directory" error.
ACM-61037	Modifyhostname.sh has relatives paths.
SF-770739 SF-583349 SF-632734 SF-681271 SF-684488 ACM-49647	Failed to create Aveksa certificate.

Issue	Description
SF-766469 SF-782885 SF-764569 ACM-61621	Aveksa ear file is not generated in /home/oracle/archive.
SF-749705 SF-757128 ACM-58548	The server takes an long time to start and migrate the .jrxml files.
SF-852928 ACM-68053	Patch does not properly migrate workflow jobs which results in display of null instead of count of workflow jobs for the review escalations.
ACM-48676	Patch installation instructions needed instructions for remote database installation. Patching script has additional checks when working with a remoted database.
SF-745721 SF-730725 ACM-59053	The requirements for a software appliance RedHat OS system were unclear.

Reports

Issue	Description
SF-741373 ACM-57697	Scheduled reports send an e-mail without an attachment when the option "Delete the report result after sending e-mail" is checked.
SF-696357 ACM-54978	Unable to run "Change Request Status Summary, by day for past month" Access Request report.
SF-787727 ACM-62247	The report was not imported properly, resulting in the bind variables Default Values not appearing on the query page of the report.
SF-777489 ACM-61686	After upgrading from 6.8.1 P20 to P22, the user sees "The request could not be handled" error in General tab when the attempting to edit or create new reports.
SF-721068 ACM-56878	User had a large report with over 65,000 lines and could not export as a usable file.
SF-792013 ACM-62488	When the user added a bind variable to the report, the resulting exported CSV file is blank.

Issue	Description
SF-856733 ACM-68359	Creating a new report that grants a user entitlements to run and view reports erroneously causes previous users to lose those entitlements.
SF-775940 ACM-61464	The Aveksa Statistics Report was reporting an incorrect number of reviewed users, accounts, and groups.

Request Forms

Issue	Description
SF-727740 ACM-56696	When a user completes an Access Request form, a validation error displays and not all values are correctly returned.
SF-822308 ACM-65213	In a custom Access Request form, when doing a search on entitlements selected from the Table Options, the selections are lost when switching to advanced search.
SF-705090 ACM-56280	When creating a Request Form and creating a new field with the type checkbox, the "off" value for the field is not set when the default value of the checkbox is set to off.
SF-791875 ACM-62506	When selected user does not populate any accounts into the table, the "User Account Table" field, in the request forms, returns a "required" warning, even though it is not configured as a required field.
SF-795918 ACM-62913	Access Request form displays L2 and L3 approvers that have been removed from the application roles.
SF-803077 ACM-63479	The User Accounts table is not displayed in forms that have a condition associated with a table, even if the condition is valid.
SF-779263 ACM-61776	When trying to run the register user request form configured with the Naming Policy having a single attribute transform, an error "Missing two input values" appears.
SF-684046 ACM-54433	Values for a drop down control in request forms cannot be deleted if the value contains quotes.
SF-859156 ACM-69165	In a Request Form, when the control type is set to Entitlement Table and the "Select only one entitlement" option is selected, the form still allows a user to select multiple entitlements.
SF-00862277	When attempting to add conditions in the display tab of an off-boarding form, the user account table and the account table with actions do not

Issue	Description
ACM-68787	display user values.
SF-851870 ACM-67724	A view table is missing the expiration date column, forcing users to look elsewhere for the information.

Role Management

Issue	Description
SF-762287 ACM-60751 ACM-62504	When a user is a member of a business role that has a technical role as an entitlement, the user is granted the technical role twice, a direct entitlement and an indirect entitlement.
SF-784859 SF-735335 SF-740094 ACM-64624	A user is granted a duplicate role when the role has a custom attribute value.
SF-780279 ACM-61688	The following error occurs when running a user access review: "ORA-20126: The creation of reviews failed. Stored Procedure:Parse_Roles_In_User_Review execution aborted. ORA-01427: single-row subquery returns more than one row."
SF-819325 SF-818430 ACM-65126	Users who match a role membership rule criteria do not match the criteria after they are removed from the role.
SF-812801 ACM-64291	The Remove action is available for a group that has been granted as an entitlement indirectly through a role under a the Access tab for a user who has the role.
SF-812781 ACM-64290	Under a user's Access tab, an entitlement indirectly granted to the user through membership in role does not indicate that the entitlement belongs to the role.
SF-812270 ACM-64693	Slow performance experienced with role management operations.
SF-813763 SF-816920 SF-818290 ACM-64568	A "Parsing failed at line" error occurred during a rule membership configuration operation for a role.

Issue	Description
SF-773391 ACM-62617	Role ownership resolved to previously deleted user.
SF-785372 ACM-62204	A terminated and then re-hired user does not match the previous membership rule for the past role.
SF-0811204 ACM-65555	Errors observed in the matching entitlements view when attempting to add an entitlement to a role in a role set that has an entitlement rule.
SF-865617 SF-858097 ACM-68704	An " ORA-30926: unable to get a stable set of rows in the source tables" error occurs when attempting to modify a role.
SF-848885 ACM-67482	Technical roles that were previously deleted are reappearing upon migration in Production.
SF-00812270 SF- 00812723 ACM-67401	When making changes to a role with 5000~ members and two entitlements, the application takes more then 20 minutes to add and commit changes, which times out in Internet Explorer.
SF-890199 ACM-70598	The size of the T_AV_ROLE_METRICS table is growing at a dramatic rate.
SF-832188 ACM-66415	Role Discovery is not working in cases where entitlement matching criteria is not specified.
SF-792647 SF-836164 ACM-65704	Role status remains in Applied or Applied New State, even after change request is complete.
SF-832126 ACM-66514	Role Definition review result lists "deleted" and "terminated" users.

Rules

Issue	Description
SF-615695 ACM-51519	Attribute change rule does not work with Unique ID condition using contains/not contains operator.
SF-800603	Rule creation with an Advanced condition expression fails.

Issue	Description
ACM-63666	
SF-764664 ACM-61365	A change request is not generated when a remediator revokes an SoD or user access rule violation entitlement.
SF-775070 ACM-64374	Inability to close a rule remediation task even though all violations for that task have already been remediated in other tasks.
SF-775070 ACM-63936	Rule violation remediator assignment missing for user access and segregation of duties rules.
SF-806515 ACM-64161	Attribute change rule action is not executed.
SF-751641 ACM-59393	The Operator, under the Update managed attribute value checkbox, does not set the value to the current date when Set to detection date is selected.
SF-777749 ACM-61791	In the Exceptional User Access Workflow, the Maintain All, Revoke All, and Clear All buttons are not functional for the Secondary Rule Remediation node.
SF-740094 SF-740342 ACM-61117	Based on the number of remediators, duplicate work items are displayed under the Violation Remediation tab.
SF-827938 ACM-66135	When a provisioning-termination rule is triggered after identity data unification, it fails to detect some terminated users.
SF-635834 SF-679132 ACM-53637	Using an advanced search filter with multiple parameters returns an error.
SF-642314 SF-765747 ACM-54369	In violation reports, some SoD violations that were given exceptional access expired prematurely.
SF-916158 ACM-72138	Rule processing fails when a rule name contains a colon.
SF-835031 ACM-66624	User entitlement attribute value is not displaying in the Separation of Duties rule violation tab, after the rule is processed.

Issue	Description
ACM-57082	The email message for the Rule Email Reminder workflow contained a typo.

Security

Issue	Description
SF-777383 ACM-61303	Specially constructed URLs could allow information leakage vulnerabilities where a user could view information for which they do not have privileges. This issue was fixed.
SF-619760 ACM-51908	The password hashes are visible in the AFX Connectors service account settings instead of the encoded asterisks.
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-933060 ACM-73252 ACM-73250 ACM-73249	Users can bypass disabled buttons in the Diagnostics screen to view, download, and delete ASRs.

Server Core

Issue	Description
SF-838469 ACM-66829	A login authorization synchronization issue is impeding users from logging on to the system.
SF-814060 ACM-64663	When completing an access request form, a warning prevents the user from saving an advanced mode query because it cannot be represented in basic mode.
SF-760448 ACM-60355	Scheduled backups are not executing automatically.
SF-677224 ACM-54028	RSA Identity Governance and Lifecycle application (version 6.9.1 P01) was unable to connect to the database with the following message observed "date: invalid date '@ERROR."

User Interface

Issue	Description
SF-816782 ACM-65559	Even though the In Table option is deselected for an attribute, it still appears in tables.
SF-799626 SF-831906 ACM-63141	A user is unable to use Shift-Click to select a range of table items.
SF-823074 ACM-67387	The Save and Continue action in a review does not refresh the whole page.
SF-819970 SF-838764 ACM-65063	The following error occurs when attempting to schedule collection by hundreds of account collectors: "UT000047: The number of parameters exceeded the maximum of 1000 at io.undertow.server.handlers.form.FormData.add(FormData.java:77)."
SF-783226 SF-803077 ACM-62595 ACM-65223	Several user interface elements are "grayed out" when using Internet Explorer after an upgrade to 6.9.1 p10. The browser used a locally cached version of JavaScript files after the upgrade.
SF-752280 ACM-60146	When writing users from RSA Identity Governance and Lifecycle through join request into an identity source, users with an apostrophe in their name get a double apostrophe.
SF-871876 ACM-69310	Fixed login code to handle when the user-agent header is not present in the request. Earlier this led to Null Pointer Exceptions in the server logs.
SF-791436 ACM-62724	In a Group Review result, previously set table defaults do not appear.
ACM-72791	Initialization status message contained a typo.

Known Issues and Limitations

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

v7.0.2 Issues

Tracking ID	Description
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-72065	Unable to open the Workflow Editor in a WebSphere clustered environment. **Workaround:** While trying to edit workflows in a WebSphere cluster, if you receive an error that indicates that the URL cannot be resolved, you may need to modify the URL used to communicate with the workflow engine. Perform the following steps to make these changes: 1. Using the File Browser, navigate to and open aveksaWFArchitect.ear. 2. In aveksaWFArchitect.ear, under /APP-INF/lib/, open acmConfig.jar. 3. In acmConfig.jar, open workpoint-client.properties. 4. Modify the property values for serverContextPath and client.connect.URL as follows, replacing *<fully-qualified-hostname>* with the fully qualified hostname and the *<port>* with the RSA Identity Governance and Lifecycle server port. • serverContextPath = http://*<fully-qualified-hostname>*:*<port>*/wpServices • client.connect.URL = http://*<fully-qualified-hostname>*:*<port>*/wpServices/xml

Tracking ID	Description
	5. Save the changes to workpoint-client.properties, and close the file.
	6. When asked to confirm whether you want to update the workpoint-client.properties file, click Update.
	7. Close the acmConfig.jar window.
	8. When asked to confirm whether you want to update the file acmConfig.jar in the archive aveksaWFArchitect.ear, click Update.
	9. Redeploy aveksaWFArchitect.ear. For instructions on deploying an .ear file, see the WebSphere Installation chapter of the *RSA Identity Governance and Lifecycle Installation Guide*.
ACM-71415	Benign exceptions report to the operating system console when installing RSA Identity Governance and Lifecycle on RHEL5U11.
ACM-63586	While a collection is running, clicking the Test Connection button on the Service Now screen for that collector fails. **Workaround:** Ensure that no collections are running before clicking Test Connection.
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.

v7.0.1 Issues

Tracking ID	Description
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-65493	When terminating a user (Users > Request > Terminate User), the associated account was not disabled.
ACM-66329	When selecting email address as a workflow variable, the Resources dialog

Tracking ID	Description
	does not show the proper variable selection.
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-67627	The Reassigned button in a fine-grained user access review is disabled after the review owner reassigns review items from one user to another.
ACM-67616	Test Connection is failing with SSL connection to an ITDS source for an account collector.
ACM-67614	The Add Resource window for a workflow node does not display the correct page number. **Workaround**: Refresh the page.
ACM-67400	The Admin menu disappears after importing metadata. **Workaround**: Log out of RSA Identity Governance and Lifecycle and then log in again.

v7.0.0 Issues

Tracking ID	Description
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 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.

Tracking ID	Description
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.