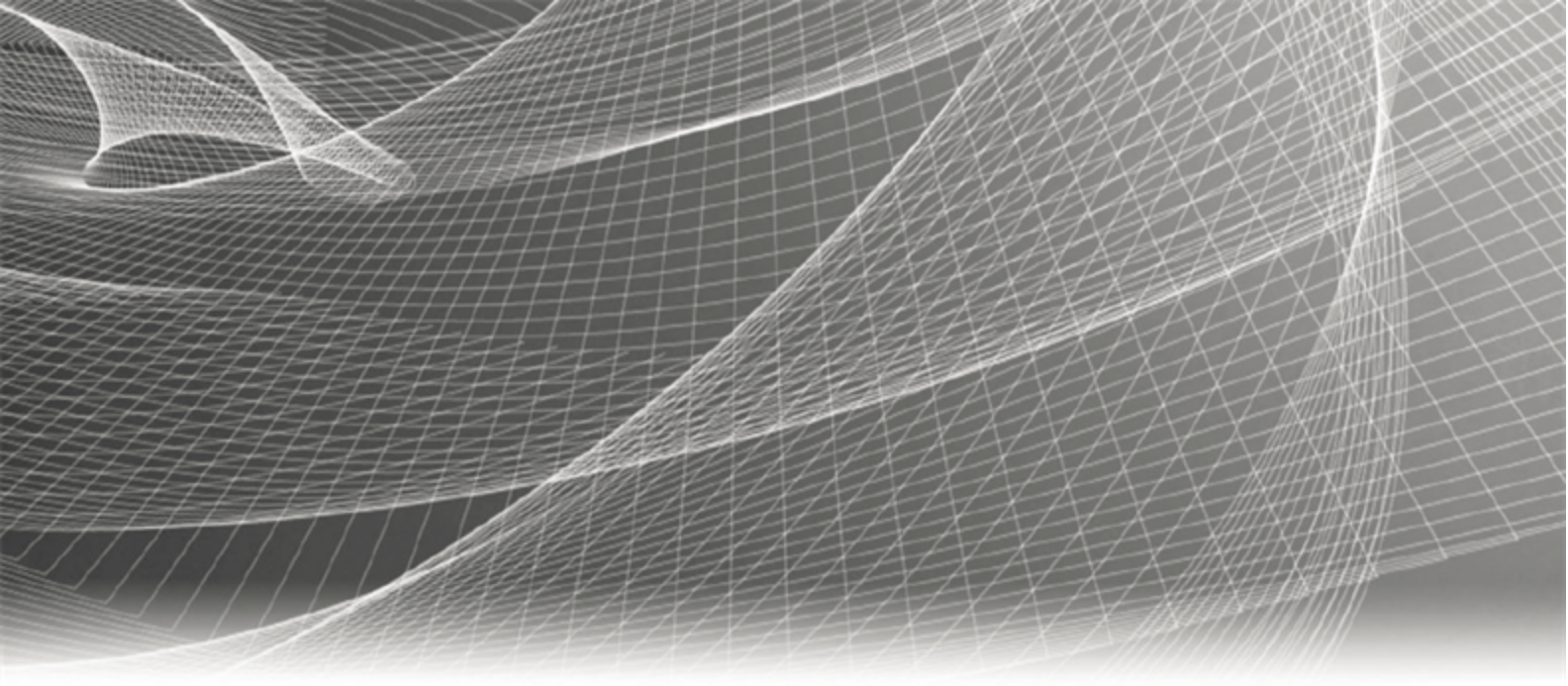

RSA IDENTITY GOVERNANCE AND LIFECYCLE

V7.1 Patch 6 Release Notes

Contact Information

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

Trademarks

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

License agreement

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

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

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

Third-party licenses

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

Note on encryption technologies

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

Distribution

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

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

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

March 2019

Contents

Supported Environments and Components

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

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

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

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

- When upgrading from product versions older than 7.1, you must upgrade to version 7.1 before you install any version 7.1 patches.

  Note: The base installation files for version 7.1 now include all improvements and fixed issues contained in RSA Identity Governance and Lifecycle 7.1 Patch 1. However, the filenames for the base installation files have not changed since version 7.1

- Do not attempt to install a previous version of a patch over a later version of a patch.
- When applying a patch in a WebSphere or WebLogic environment, you must uninstall the Workflow Architect EAR before applying updates.

Before you begin

- Customizations made using the RSA Identity Governance and Lifecycle user interface are preserved during the upgrade process. However, any customizations made directly to the EAR are overwritten during the patching process. If you have made any customizations to the EAR, record the customizations before performing the upgrade, and manually restore them after you complete the installation.
- The way in which RSA Identity Governance and Lifecycle handles business descriptions for groups has changed from previous product versions.

  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 on page 11.

- If your environment uses a 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 an RSA-supplied database, the patch script automatically stops and starts the 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.
  For additional details for WebSphere and WebLogic environments, see the*RSA Identity Governance and Lifecycle Installation Guide*. For additional details for WildFly environments, see the document *Configuring WildFly Clustering*.

- **Note:** The created product schemas, such as AVUSER, are reserved for product database objects.

Creating additional database objects within the product schemas may affect the operation of the systems, migration, or patch applications.

Migration Queries for Group Business Descriptions

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

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

Unused Group Business Descriptions Not Associated with an Application

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

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

```
    )
AND a.scope_id IS NULL
AND a.is_deleted = 'FALSE'
AND a.object_type = 4
AND a.applies_to_set = 'FALSE';
```

All Unused Group Business Descriptions

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

```
SELECT
    id,
    'Group' as Type,
    object_filter AS "Object Filter",
    alt_name AS "Display Name",
    short_desc AS "Short Description",
    long_desc AS "Long Description",
    url_ref as "Help Link",
        (select name from t_groups where id =
        a.scope_id) as "Group Name",
        (select name from t_applications where id =
        a.scope_id) as "Application Name"
FROM
    t_av_business_description a
WHERE
    NOT EXISTS (
        SELECT
            application_id
        FROM
            t_groups b
        WHERE
            b.filter_id = a.id
        )
```

```
AND a.scope_id IS NOT NULL
AND a.is_deleted = 'FALSE'
AND a.object_type = 4
AND a.applies_to_set = 'FALSE';
```

Group Business Description Table

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

```
declare
v_tbl_count number;
Begin
     select count(*) into v_tbl_count
     from user_tab_columns
     where table_name = 'TEMP_BUSDESC';
     if v_tbl_count > 0 then
     execute immediate 'drop table temp_busdesc purge';
     end if;
     execute immediate
     'CREATE TABLE temp_busdesc
          AS
               SELECT
                    name,
                    id,
                    filter_id,
                    application_id
               FROM
                     t_groups
               WHERE
                     filter_id !=-1';
end;
```

/

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
        - For WebSphere: ACM-WebSphere-<*VersionNumber*>_P<*PatchNumber*>.tar.gz
        - For WebLogic: ACM-WebLogic-<*VersionNumber*>_P<*PatchNumber*>.tar.gz
      - upgradeJDK<*version*>_<*revision*>.tar (optional JDK update for security updates)

3. If this release does not include a new JDK version, this step is optional. If you have already applied the latest JDK version, there is no need to reapply it. Apply the JDK upgrade as follows:
   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. Install the patch:
   - In a WildFly environment:
     a. Log in as root and run the patch.sh installation script in the directory created in Step 4. Run the following commands:
        i. cd /home/oracle/Aveksa_<*VersionNumber*>_P<*PatchNumber*>
        ii. sh patch.sh
     b. When the patch script completes, restart RSA Identity Governance and Lifecycle. Run the following command:

        ```
        acm restart
        ```

   - In a WebSphere or WebLogic environment, perform the following steps to apply the patch. For detailed instructions, see the*RSA Identity Governance and Lifecycle Upgrade and Migration Guide*.
     a. Perform any necessary customizations to the Aveksa EAR and Workflow Architect EAR files. For more information, see "Modifying the RSA Identity Governance and Lifecycle Enterprise Archive" in the *RSA Identity Governance and Lifecycle Installation Guide*.
     b. Uninstall the Workflow Architect EAR.
     c. Upgrade the Aveksa EAR.
     d. Deploy the Workflow Architect EAR.
     e. Restart the WebSphere or WebLogic Application Server.

After you finish

- 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.

  To stop and restart RSA Identity Governance and Lifecycle in a WebLogic environment:

1. In the WebLogic administrative console, select **Deployments** from the menu.
2. Select the Aveksa application and click **Stop** and then **Start** to restart the application.

   Restarting RSA Identity Governance and Lifecycle also restarts the local agent.

- If your deployment includes Access Fulfillment Express (AFX), you must also upgrade your AFX connectors. For instructions, see Download and Import AFX Connector Packages on page 16.

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 7.1 Patch 6

Information about the 7.1 Patch 6 release is included in the following sections:

User Interface and Behavior Changes in Release 7.1 Patch 6

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

Issue	Description
Access Certification ACM-93895	If a reviewer attempts to save or sign off changes while their earlier changes are processing, the user interface now displays a warning message that indicates that the review has another save or sign off in progress, and that the user can submit the changes after the previous changes have completed.
Access Requests ACM-92751 ACM-93823	The default out-of-office functionality will now process Global Common Submission Questions to complete a request submission.
Change Requests and Workflows ACM-95063	A workflow form not successfully deleted will prompt an error in the user interface.
Change Requests and Workflows ACM-95214	The conditional transition selection now saves properly through the drop-down selection button.
Metadata Import/Export ACM-92269	The application metadata now exports information about mapped connectors. When the metadata is imported, if the specified connector is available, the application is mapped to the connector.
Security ACM-94695	Only users with edit privileges can view the debug properties and configuration for REST and SOAP Web Service nodes.
User Interface ACM-92551	To improve performance, a user interface table no longer calculates the number of items in a change request for each listed task.

Fixed Issues in 7.1 Patch 6

The following issues were fixed in RSA Identity Governance and Lifecycle version 7.1 Patch 6.

Access Certification

Issue	Description
SF-1262429 ACM-92238	The Member, Entitlements, and Analytics tabs of a role could not be clicked in a role review with "submit" as the mandatory signoff comment.

Issue	Description
SF-1090220 ACM-83577	The "Explicit by Owner" option in the Account Access and Ownership review, when sub-components were automatically revoked through a revoked parent component, caused incorrect confirmation messages after canceling review changes.
SF-845541 ACM-67727	The "Apply to account entitlements" option for bulk actions did not work on associated app roles and entitlements in an account review due to a column filter in a custom review display view.
SF-1300767 ACM-94654	The Account Name column was missing from the available columns to display in a review display view.
SF-1170335 ACM-87413	Could not send emails using the Send Email button in the All Groups tab of group reviews.
SF-1150335 ACM-93895	Reviewers attempting to save or sign off changes while their earlier changes were still processing saw the following error message: "The request could not be handled."
SF-1307372 ACM-87205	Localization in the new reviewer user interface required multiple improvements.

Access Requests

Issue	Description
SF-781743 SF-856286 SF-872111 ACM-61578	Change requests with fulfillment dates set later than 2040 were erroneously fulfilled immediately.
SF-1290694 ACM-94018	The ${avform.requestor.Id} variable did not resolve as expected for **users.Supervisor** and grayed out the associated button due to the resulting sql error.
SF-1260207 SF-1290214 ACM-92751 ACM-93823	The default out-of-office functionality failed to process Global Common Submission Questions when configured.
SF-843249 ACM-67217	When a user viewed a request form with table grouping enabled, the list of entitlements took much longer than expected to expand if the checkbox next to the entitlement type was selected.

Account Management

Issue	Description
SF-1191999 ACM-89978	The AFX output parameter did not update the pending account, even though AFX received the value from the endpoint.

Admin Errors

Issue	Description
SF-1205426 ACM-90188	Email failures did not appear in the notification tray to alert the admin.

AFX

Issue	Description
SF-936411 ACM-73373	AFX erroneously resent requests that had previously failed or been canceled.

Application Wizards

Issue	Description
SF-1073265 ACM-82980	Custom Value List display names were not allowed in an advanced search with Integer Type attribute filtering.

Change Requests and Workflows

Issue	Description
SF-1284183 ACM-93525	A fix applied in an earlier patch for change requests stuck in the fulfillment phase stopped working after an upgrade.
SF-1293969 ACM-94160	The AFX create account action failed when a change request with multiple "Create Account" items for multiple applications and for a single user has one of the "Create Account" items rejected.
SF-1292210 SF-1228815 ACM-94109	Role approvals grouped by a custom category mixed up the acm.JobGroup values assigned in the workflow to define the group.
SF-1307962 ACM-95063	A new workflow form for an activity or approval did not associate to its respective node when saved and did not replace the previous form as a result.
SF-1279390 ACM-93461	Corrupted mapping for provisioning command parameters occurred after an upgrade.
SF-1314848 ACM-95214	The conditional transition selection failed to save the first time when setting the condition through the drop-down selection button.
ACM-94082	Could not delete an escalation that referenced an escalation workflow that did not exist from the approval node.
SF-1274945 ACM-92854	When a change request was created with an entitlement that had a business description, the short and long business descriptions appeared empty under User Changes in the change request approval screen.
SF-1155926 ACM-87274	Additional Javadoc was needed about the use of Java nodes in workflows.
SF-1255736, SF-1279531, SF-1349690, SF-1332507 ACM-91858	After importing a workflow from a higher patch version into a lower patch version, migration failed with the ORA-0001 error.

Collector

Issue	Description
SF-1299910	The Salesforce ADC was missing attributes listed in the datasheet.

Issue	Description
ACM-94323	
SF-1298037 ACM-94661	The ServiceNow collector failed after certain plug-ins were activated.
SF-1273747 ACM-93287	The Office365 PowerShell Collector took an excessively long time to complete.

Dashboard

Issue	Description
SF- 938836, SF-1082693 ACM-74513	Secondary pages of a report displayed within a dashboard were not displayed properly.

Data Collection Processing and Management

Issue	Description
SF-1260229 ACM-92496	Unification failed with unknown error after an upgrade.
SF-1300333 ACM-94263	Running two MAEDCs failed with error ORA-30926 if they overlapped in applications and IDs.
SF-1187676 ACM-89996	Users could not login during the first step, Account Data Collection, of a running ADC.
SF-1249962 ACM-91612	Change Verification performance slowed on large datasets after an upgrade.
SF-1312017 ACM-94871	The App Metadata collector trimmed values longer than 38 characters for owner and CAU fields.
SF-1217455 ACM-89969	Indirect relationship processing ran for more than 5 days after changes to the MAEC.
SF-1216820 ACM-92280	The provided fix to truncate the T_AV_BUSINESS_DESCRIPTIONS table did not successfully shorten the long collection time.

Data Governance

Issue	Description
SF-1302256 ACM-94318	Data purging failed with the ORA-02292 error "integrity constraint (AVUSER.FK_T_PCS_EXN_HY_PC_ID_T_PCS_ID) violated - child record found".

Database Management/Performance

Issue	Description
SF-1246819 ACM-93524	A database import process generated unneeded statistics for certain tables.
SF-1297442 ACM-94181	The "Provisioning screens for 50 users" performance test showed an unoptimized sql query.

Email

Issue	Description
SF-824105 SF-1006954 ACM-65511	The Review Completed event sent emails only to reviewers with open items.
SF-803604 ACM-64365	The View Review hyperlink to a deleted review result in a New Review email incorrectly showed the error "The Request could not be handled."
SF-1300504 ACM-94697	Case-sensitive email approvals resulted in "Wrong user replied" responses when taking an approve or reject action through email.
SF-1155182 ACM-88160	Lotus Notes could not correctly display Nordic characters in emails sent by RSA Identity Governance and Lifecycle.

Metadata Import/Export

Issue	Description
SF-1257224 ACM-92539	Performance slowed for importing or modifying an application with a large amount of users.
SF-1230774 ACM-92269	An application that was imported from an exported metadata file was missing information about mapping the application to a connector.

Migration

Issue	Description
SF-1341007 ACM-96450	Updating RSA Identity Governance and Lifecycle 7.1.0 through 7.1.0 P02 to 7.1.0 P03 through 7.1.0 P05 failed with the following error: java.lang.ClassNotFoundException: com.aveksa.migration.db.password.ViewPasswordSettingMigrator.

Password Management

Issue	Description
SF-1177525 ACM-87860	In a clustered environment, the PasswordResetNag and PasswordChangeNag tasks could be duplicated and cause a startup error.

Platform

Issue	Description
SF-642369 ACM-52522	Changes to the root logger level in a clustered environment failed to apply to all associated nodes.
SF-1019541 ACM-78253	After running the HardenHTTPSProtocols.sh script in the /home/oracle/deploy directory, the following warning occurred: "WARN: can't find jboss-cli.xml. Using default configuration values."

Reports

Issue	Description
SF-1158510 ACM-93535	Two OOTB report templates, Changes in User Global Roles by Date Range and Changes in User Global Roles in the Last n Days, worked only for collected role changes and not

Issue	Description
	local role changes.
SF-1261751 ACM-93822	The report query processed the < character as HTML mark-up code and truncated text that followed it.
SF-1163099 ACM-86916	When using the replace function during a preview or submission, special characters were removed from queries.
SF-1190029 ACM-88495	Query parameter detection did not work properly with an unmatched single quotation mark in the comment.
SF-986549 ACM-78252	A request form vulnerability showed authorizations that a user should not be able to request.
ACM-89680	When a user tried to view a report that was no longer available, the following incorrect error message was displayed: "Access Denied. Insufficient privileges to view this page."

Request Forms

Issue	Description
SF-1300030 ACM-94292	The User picker control type reports an SQL exception error when the user filter is enabled and no variable substitution is defined in the filter.
SF-1310845 ACM-94989	Variable substitution in the control type "Drop Down with Web Service" did not encode for javascript.
SF- 1201270 ACM-88959	After a button was configured to include forms of multiple form types, only global forms were displayed when the button was pressed.

Role Management

Issue	Description
SF-1158276 ACM-86615	An indirect entitlement provided through a role could erroneously be removed while comparing users.

Rules

Issue	Description
SF-1264397 ACM-93893	When the UCD rule detected an orphan account, an email was sent to a random supervisor if no supervisor was associated to the account.
SF-1322268 ACM-95316	The Attribute Change rule skipped users when multiple Rule runs were queued.

Security

Issue	Description
SF-1307234 ACM-94695	Sensitive info in REST and SOAP Web Service node configuration could be viewed by users without edit privileges.
SF-1158051 ACM-86836	The status page shown at the end of the password reset process needed a sanitized URL.

Issue	Description
SF-1284851 ACM-93533	Needed to update the Apache Commons jar to the most recent version to increase security.
SF-1158051 ACM-86955	Additional validation and sanitization was needed for the file upload functionality in access requests.

Server Core

Issue	Description
SF-1257836 ACM-93038	Scheduled Unification was triggered before the scheduled IDC run and caused the incorrect processing of rules.

User Interface

Issue	Description
SF-1233063 ACM-91269	The database view V_ROLE_TO_APPS did not include local roles in addition to collected roles.
SF-1257307 ACM-93514	The UI became unresponsive when using French language settings.
SF-1251232 ACM-92551	The load time for Review pages and Request Activity pages slowed after an upgrade.
SF-1310137 ACM-94849	After a data retention job runs, the Change State column in the Activities view could not display some of the remaining data.
SF-1193085 ACM-88580	The user interface did not notify that a previously uploaded .jsp file reloaded with modifications required a server restart for the changes to take effect.
SF- 1167740 ACM-92498	In a dashboard, the complete name of a request button was not fully visible.
SF-630081, SF-680821 ACM-54208	When a user submitted a request, the Select Request Source screen displayed incorrect business source attributes.

Web Services

Issue	Description
SF-108829 ACM-87443	Online documentation for the createChangeRequest webservice needed to clarify when the change request is not created.

Release 7.1 Patch 5

Information about the 7.1 Patch 5 release is included in the following sections:

What's New in Release 7.1 Patch 5

Feature	What's New
Request Forms ACM-89196	The Entitlement Table, Entitlement Table with Action, and Entitlement Table (non-visual) request form controls can now filter entitlements by entitlement types: entitlements, groups, roles, and application roles. This allows a finer scope and improved performance for the request form controls when only specific entitlement types are needed.

User Interface and Behavior Changes in Release 7.1 Patch 5

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
Admin Errors ACM-92855	The Admin Error type "Account Load Data" can now contextually appear in the properties of a Create Admin Error workflow node.
Change Requests and Workflows ACM-88351	The Show Job Level Variables setting in request workflows will not overwrite the same setting in approval and fulfillment workflows.
Change Requests and Workflows ACM-88384	A workflow must be removed from configuration (phase nodes, subprocesses, and escalations) before it can be deleted.
Change Requests and Workflows ACM-89649	The Business justification character limit has increased to 4000 while editing exceptional access.
Change Requests and Workflows ACM-93462	The "Assign to" list no longer appears as available options for Resource Selection.
Data Collection Processing and Management ACM-90663	The date range of historical configuration information has been reduced in areas such as collector changes.
Data Collection	The Last Reviewed Date OOTB attribute has been removed from the collector wizards.

Issue	Description
Processing and Management ACM-91761	
Role Management ACM-87106	The Out of Constraint Users list in the Analytics tab has changed to use the same format as the Users list in the Users tab.
Web Services ACM-92041	Validation for webservice calls to add or remove accounts from a group can be requested using the collector or the business source, but not both.

Fixed Issues in 7.1 Patch 5

The following issues were fixed in RSA Identity Governance and Lifecycle version 7.1 Patch 5.

Access Certification

Issue	Description
SF-1157646 ACM-86823	Reviews erroneously generated sign off reminder emails when reviewers were not allowed to sign off for themselves.
SF-1176460 ACM-87929	A reassigned review configured to allow a delegated user to sign off did not enable a delegate to sign off as intended.
SF-1173057 ACM-88464	Account reviews that generated change requests explicitly by owner did not properly create revoke item change requests if application business owners and directory technical owners were granted monitor access.
ACM-88164	A fine-grained role review for bulk revokes of role memberships with large user counts performed slower than expected.
ACM-92706	A bulk revoke action during a fine-grained role review on a role's user member or entitlement that was already revoked caused an error.
SF-1178009 ACM-90758	A reviewer listed in the Escalations Tab could not be found by the search tool.
SF-1172039 ACM-87438	Some reviewer escalation workflows were not triggered and the review history did not update if the review became active by an escalation workflow.
SF-1176983 ACM-88167	The Radio button text "Review items are signed off" on the configuration page of a User access review definition appeared when the sign-off option was not actually available.

Access Requests

Issue	Description
SF-1156659 ACM-86562	The Entitlement View did not filter correctly as instructed by "Initial set of entitlements to show" when triggered by a request button.
SF-1189546 ACM-92989	An added submission field did not appear in Additional Information while creating a Change Request for an application with groups.
SF-1286545 ACM-93599	A "Remove account to group" change request from a webservice did not set the affected users in the request information.

Issue	Description
SF-1193655 ACM-89679	If a user closes the browser or navigates away from the page using any function other than the cancel or back buttons, entries for pending accounts are left in T_AV_ ACCOUNTS.

Account Management

Issue	Description
SF-892981 SF-1103183 ACM-71073	The Who Has Access tab did not display any users.

Admin Errors

Issue	Description
SF-1223251 ACM-90384	A Notification rule that used Identity Unification as an error source did not send an email to the specified users as expected.
SF-1265089 ACM-92855	The Account Load Data error was not listed for available types in the properties of a Create Admin Error workflow node.
SF-1205426 ACM-90188	Email failures did not appear in the notification tray to alert the admin.

Authentication

Issue	Description
SF-1215963 ACM-90219	The Active Directory objectGUID and objectSID were not properly supported attributes from authentication sources for either account or identity data collection.

Aveksa Statistics Report

Issue	Description
SF-1138522 ACM-85418	Decision Node settings changed automatically in the Out of Office workflow when any other node was changed and saved.

Change Requests and Workflows

Issue	Description
SF-1173926 ACM-88384	Custom workflows could not be deleted.
SF-1158316 SF-1204062 ACM-90489 ACM-90603	Workflow variable names showed unexpected format changes after an upgrade.
SF-1204867 ACM-89649	When editing existing exceptional access, the user interface limited the business justification to 500 characters while it allowed 4000 characters for new entries.
SF-1258377 ACM-92069	After applying a patch, Workflow SQL nodes periodically failed with null pointer exceptions.

Issue	Description
SF-1222578 ACM-90665	The variable value ${access_request_cri_app_cas2} did not successfully populate after a patch was applied.
SF-1230171 ACM-90666	On restart, a Change Request with only form fulfillment created a workflow that skipped all its form fulfillment nodes.
SF-1277646 ACM-93113	Parallel Phase Nodes duplicated workflow and fulfillment jobs because of concurrency errors.
SF-1277724 ACM-92992 ACM-92993	The REST Node POST request body mandated XML code that was not required.
SF-1161187 ACM-90147	An Errors link in the run history of a Custom Task job summary table did not show the logged errors when clicked.
SF-1266678 ACM-93462	The "Assign to" list incorrectly showed as an option for Resource Selection.
SF-1294015 ACM-94309	The Jobs tab in Admin > Workflow showed a UI error when evaluating errors with over 4000 characters.
SF-1304407 ACM-94532	A subprocess node condition applied to nodes without following configured settings.
SF-1297357 ACM-94126	The Group by Category approvals were skipped in Joiner workflows.
SF-1181059 ACM-88351	The Show Job Level Variables setting in request workflows overwrote the same setting in approval and fulfillment workflows.
SF-1293969 ACM-94160	The AFX create account action failed when a change request with multiple "Create Account" items for multiple applications and for a single user has one of the "Create Account" items rejected.

Collector

Issue	Description
SF-1305102 ACM-94653	CSV database processing could not handle column header values nested in double quotation marks.

Connector

Issue	Description
SF-1214862 ACM-89813	The ServiceNow AFX Connector lacked command output parameter settings for the "Check Ticket Status" and "Check Request Status" capabilities.

Data Collection Processing and Management

Issue	Description
SF-831492 ACM-89647	Duplicate users appeared in the data when a deleted user from an earlier version was recreated with the exact same settings.

Issue	Description
SF-1224169 ACM-91121	Collection added duplicate Aveksa access entitlements to the account and user.
SF-1228554 ACM-90663	A data table stored historical configuration information in clear text.
SF-1201069 ACM-89785	Duplicates created in the T_SCHEDULED_TASKS table prevented unification from completing.
SF-1231311 ACM-91584	Unification removed user account mapping when one of many resolution attributes was changed.
SF-1236885 ACM-91586	An ADC User Resolution with more than 3 attributes from the same source left an account unmapped and without an ORPHANED_DATE value.
SF-1242815 ACM-91761	The Last Reviewed Date OOTB attribute erroneously showed as an available collector mapping attribute in the UI.

Database Management/Performance

Issue	Description
SF-1224207 ACM-90323	A Data purge job that ran through the backend repeatedly failed to complete the custom task purge.
SF-1201744 ACM-89849	Performance issues occurred when revoking entitlements from a role during a fine-grained role review.
SF-1074740 ACM-85409	An error occurred after a CLOB was converted into a varchar in the CHANGE_REQUEST_VARIABLE view.
SF-1203774 ACM-88976	Performance issues occurred when editing roles.

Email

Issue	Description
SF-1191611 SF-1240924 ACM-88807	Some Approval Email replies did not show the correct reference numbers for a request and showed <AV-MsgRef-REF> instead.
SF-1056837 SF-1155367 ACM-80572	A requestor still received approval emails despite being on the Exclude list.

Installer

Issue	Description
SF-1205479 ACM-89296	The Database-Only installation did not check for sufficient disk space to complete installation.

Password Management

Issue	Description
SF-1196317 ACM-88868	The special character "<" was trimmed from the password field if it followed a number in the character string.

Reports

Issue	Description
SF-1219878 ACM-90510 ACM-90511	The T_AV_AFX_LOG_MESSAGE and T_EMAIL_LOG tables lacked a public view of their data.
SF-1271093 ACM-92667	Scheduled reports in XLS-format could not be opened after migration.
SF-1258049 ACM-92226	After an upgrade, reports using the PV_USER_ALL_ACCESS view failed with an error if the report had custom value integer attributes.
SF-782401 ACM-63770	After applying a style template to a report or report template, the Apply Style Template to Report screen did not indicate the currently applied style.
SF-1219878 ACM-90512	The tables T_AV_AFX_REQUEST & T_AV_AFX_REQUEST_HISTORY did not contain public views.
SF-1158510 ACM-88913	The OOTB report using the template "Changes in User Global Roles by Date Range" could become stuck due to excessive query executions.
SF-1284789 SF-1291139 ACM-93688	CSV Column headers were duplicated when exported as an attachment in an email from a scheduled report generation.
SF-1130030 ACM-88494	A Report with a non-standard column defined with TO_DATE/TO_TIMESTAMP functions in a select statement could fail to extract the date and showed the "jasperreports.engine.JRRuntimeException" error instead.
SF-968478 ACM-76164	When a form was designed with an application name that did not match the business source raw name, the account filter did not work correctly.

Request Forms

Issue	Description
SF-1194256 ACM-88878	The Display and Enabled conditions for an entitlement table did not work as expected.
SF-1239355 ACM-91122	The conditions to display or enable an entitlement table form control could not be properly verified in the form.
SF-912473 SF-957890 ACM-72112	The request form did not properly validate a direct request for entitlements that were already granted indirectly through a role.
SF-1263329 ACM-92257	A request form associated with a business source could not be edited because of an error.

Issue	Description
SF-1212317 ACM-90015	Email sent with an External URL link that contains the externalURL and title parameters caused "request could not be handled" errors.
SF-1212748 ACM-91669	The entitlement table with display conditions did not appear when the dynamic variable value changed.

Role Management

Issue	Description
SF-1166227 ACM-87106	On the Analytics tab, the Out of constraint user table disappeared and the UI locked up and displayed incorrectly when a user was removed from the table.
SF-882193 ACM-70716	When creating roles using the Discover Roles functionality, the suggested entitlements do not match the suggested entitlements condition.

Rules

Issue	Description
SF-1180940 ACM-88634	A Termination Rule with the 'or' condition for a Delete Accounts action did not create the expected change requests to revoke entitlements.
SF-1080104 SF-642932 ACM-52576	The termination rule created a duplicate request that could not be completed when a user was terminated and then deleted.
SF-1000621 SF-1041352 SF-1100872 ACM-77042	Scheduled rules ran multiple times when the rule name or type had been changed.
SF-1262986 ACM-92256	The User Access Rule only worked when applied to a single user.

Security

Issue	Description
SF-1213459 ACM-90322	The patch includes an updated version of JDK 8, which addresses some known security vulnerabilities. **Note:** Follow the instructions in Install a Patch on page 10 to update the JDK.
SF-1223436 ACM-91372	Users granted the "View All" role could not see group and role members in the What Access tab.
SF-1022650 ACM-78259	Applied properties to enhance security for an internal communications port used by a mule agent.

Server Core

Issue	Description
SF-1128205 SF-1144286	Heavy change request activity increased the ADC processing time for longer than expected.

Issue	Description
SF-1159804 ACM-84894	

User Interface

Issue	Description
SF-1158799 ACM-86788	The Accounts table in the Directories Resource Accounts Tab showed a "Backup Supervisor" column in Table Options that is never populated in an accounts table.
SF-1072223 SF-1080714 ACM-83584	Multiple clicks on a form could select one item multiple times to create duplicate selections.
SF-969882 ACM-75372	The notification button opened a blank window with a disabled Complete button if no tasks were available to the user.
ACM-92994	Proxy protocol changes in a Rest Node could not be saved.
SF-1176345 ACM-88381	The node filter in System > Logs could not show any logs in a WebLogic environment.
SF-1042710 ACM-79980	The log page in Admin > Email did not show results correctly when sorted by Processing Result.

Web Services

Issue	Description
SF-1253334 ACM-92041	Duplicate group names on a multi app collector could cause the webservice call that created a change request to choose the wrong group.
SF-983571 SF-1223579 ACM-76016	The User Attribute Change webservice reported a "User Not Found" error when the User ID was on record.
SF-1264262 ACM-92518	The documentation for the processRule Web Service did not state that a token was mandatory.

Release 7.1 Patch 4

Information about the 7.1 Patch 4 release is included in the following sections:

What's New in Release 7.1 Patch 4

Feature	What's New
Change Requests and Workflow	Upgrade of Workflow Engine to 4.40.16.

User Interface Changes in Release 7.1 Patch 4

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

Issue	Description
Access Certification ACM-88680	The "Save Tab in Table" option has been removed from table pop-ups.
Change Requests and Workflows ACM-88211	Workflows cannot be selected across different types of modules and are only selectable for the appropriate module type.
Change Requests and Workflows ACM-89833	The fulfillment workflow now uses the correct query to group fulfillments by business source.
Change Requests and Workflows ACM-89860	WorkItemURL selection is now available for manual nodes.
Change Requests and Workflows ACM-90476	A custom task must be removed from the schedule before it can be deleted.
Data Collection Processing and Management ACM-81403	If an agent cannot resolve the Member Type from the Account Data Collector's source system for a group's member, it assigns "unknown" to the Member Type column in the raw data instead of guessing the correct member type. When Member Type is "unknown", the collector's database processing still attempts to resolve the member type. If successful, it assigns a member type in the new "Resolved Member Type" column in the raw data. If Member Type is "unknown" and the member type cannot be resolved by the account collector, then Resolved Member Type is left blank and the collected membership is rejected.

Issue	Description
Installer ACM-87123	Applying a patch overwrites the configuration files for plugins except for the ITIM2FulfillmentHandler, NovellIMListener, and SunFulfillmentHandler plugins, which are copied from the customer's system instead. The patch application process backs up the original plug-in configuration files in the folder **<location of the patch>/backup/<timestamp>/plug-ins/** so that you can restore them if needed.
Role Management ACM-74637	The "Role Missing Entitlement Rule" email notification now adds group entitlements collected from the ADC.
Rules ACM-90043	An "Associate Remediation Job" button has been added to the Rule Details page for remediation actions. When clicked, remediation workflow jobs are created for identified and unassociated violations. This button is not enabled by default, but can be enabled by the "ViolationRemediationReProcess" feature flag.

Fixed Issues in 7.1 Patch 4

The following issues were fixed in RSA Identity Governance and Lifecycle version 7.1 Patch 4.

Access Certification

Issue	Description
SF-1190649 ACM-88508	The global table options for filters, groups, and columns did not work for the Reassign and Share Review functions in the new User Access Review interface.
SF-1195963 ACM-88680	A reviewer without required privileges could download the full list of users and attributes from any User Picker pop-up.
SF-1205481 ACM-89536	A privilege column added to the reviewer coverage file of an account review definition did not appear in a .csv file saved from the data.
SF-1239517 ACM-91180	Review Generation for large datasets slowed in performance after an upgrade.

Access Requests

Issue	Description
SF-1044261 ACM-79614	Several entitlements were removed at once when only one entitlement was requested for removal.
SF-1162322 SF-1171080 SF-1185324 ACM-75782	A change request could not be performed because it misnamed the account name for the requested entitlements.
SF-1223556 ACM-90304	When reverting a pending account, an Oracle error "ORA-19279" prevented successful completion of the action. Also, restarting RSA Identity Governance and Lifecycle while some change requests were not finalized could result in the same Oracle error "ORA-19279" and prevent server initialization that resulted in users not being able to log in.
SF-1189389 SF-1189398 SF-1189404	The system did not generate change requests from violation remediation actions for revoked accounts when simultaneously revoking and giving exceptional access for multiple accounts that belonged to the same app role.

Issue	Description
ACM-88467 ACM-88468 ACM-88477	

Aveksa Statistics Report

Issue	Description
SF-810446 SF-834464 SF-1078132 SF-1183919 ACM-64920	A null pointer exception error occurred when creating an ASR with "Include database performance statistics" enabled.

Change Requests and Workflows

Issue	Description
SF-1059087 ACM-81419	Canceling a change request that added a role with entitlements or groups reverted the role but did not remove indirect entitlements.
SF-1168903 ACM-89833	A change request generated from a termination rule bypassed a custom fulfillment workflow.
SF-1217300 ACM-89860	The URL parameter variables ${ValidReplyAnswers} and ${WorkItemURL} did not show in the workflow design page as available shortcuts.
SF-981092 ACM-84977	The decision node for workflow conditions on a request escalation was always set as "true".
SF-1192314 ACM-90476	A custom task could not be deleted if it was scheduled.
SF-1258377 ACM-92069	After applying a patch, Workflow SQL nodes periodically failed with null pointer exceptions.
SF-01171991 ACM-88211	Non-Access Request workflows had inconsistent behavior dealing with Activities.

Collector

Issue	Description
SF-1185812 ACM-88921	An LDAP search initiated by RSA Identity Governance and Lifecycle asked for the same AD attribute multiple times if it was mapped to more than one of the attributes for RSA Identity Governance and Lifecycle.
SF-1190006 ACM-88607	When testing a role collector query, syntax errors occurred.

Connector

Issue	Description
SF-1205499 SF-984004	After performing a migration, the Federated Salesforce connector template and Microsoft Exchange connector template remained in a migration required state.

Issue	Description
SF-1051212 SF-836060 ACM-89197	

Data Collection Processing and Management

Issue	Description
SF-1193983 ACM-88706	The Role Data Collector failed with an Oracle error that reported unstable rows in the source tables.
SF-1213227 ACM-89674	The Account Data Collector could not call custom code prior to loading the raw data.
SF-1197266 ACM-88960	Any unprivileged user could export or save data in a table displayed within a pop-up.
SF-1220029 ACM-90277	Manually mapping a user account submitted a new indirect relationship processing job whether or not the job was already in queue.
SF-1062777 SF-1020344 SF-1108676 SF-1213238 SF-1224190 SF-1219428 ACM-81403	Group collection rejected the nested group relationships and misidentified groups as accounts when listed as members of other groups.
SF-1175678 ACM-87948	Collections from a .csv file returned too many rows after an upgrade.

Database Management/Performance

Issue	Description
ACM-90149	A backup started with a backup already in progress stopped with a warning but did not return with a failed status.
SF-892279 SF-1068981 SF-1186911 ACM-72284	The PV_USER_DIRECT_ACCESS view did not have a join condition on the entitled ID to show correct information.
SF-1190864 SF-1190863 ACM-88534	Slow SQL query performance occurred after upgrading from version 6.9.1.
SF-1128305 ACM-85934	User interface page-loading time and collections took an unusually long time.

Descriptions

Issue	Description
SF-1209242	During the import of business descriptions, the status pop-up that appears when

Issue	Description
ACM-89625	importing business descriptions did not appear when choosing to overwrite or skip existing entries.

Email

Issue	Description
SF-1038728 ACM-79982	The user interface became unresponsive when an emailed tabular report bounced due to size limitations of the recipient's mailbox server and the aveksaServer.log file recorded the email along with the entire attachment in encrypted format.

Installer

Issue	Description
SF-1166648 ACM-87123	After patching RSA Identity Governance and Lifecycle, the user interface did not display an Edit button for the Email Fulfillment Handler as expected.
SF-1193541 ACM-88761	The oracle error "ORA-30657: operation not supported on external organized table" occurred when applying an upgrade or patch.
SF-973587 ACM-75344	The Patch installation process did not stop to show an error message when an issue occurred with the archived .ear file.

Metadata Import and Export

Issue	Description
SF-1077965 ACM-82017	Incorrect error message was displayed when importing a rule with an invalid global role reference.

Migration

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

Password Management

Issue	Description
SF-1173793 ACM-88150	The current password could not be validated against a stored password history hash during a password change.

Reports

Issue	Description
SF-882602 ACM-71754	An Out of Role Entitlements report did not show the expected results.

Request Forms

Issue	Description
SF-1038696 ACM-79773	The form did not correctly show certain colors to highlight target users depending on their access.

Role Management

Issue	Description
SF-911444 ACM-77583	Terminated users were erroneously granted indirect role memberships when they were still part of a role that added an entitlement.
SF-927983 ACM-73210	Role Discovery stalled and timed out on a database query when using a high-load HASH-JOIN view on the GTT_CLUSTER_ENT_COUNTS table.
SF-901924 ACM-73623	A specific role showed a "could not execute query" error in the user interface instead of the role data.
SF-1213844 ACM-90265	A null pointer exception error occurred when viewing the Out of Constraints users section in Analytics if "Remove" is the only column in the table.
SF-950510 ACM-74637	The "Role Missing Entitlement Rule" email notification did not include the group entitlement collected from ADC. Code was missing to add the group entitlement to the email notifications.

Rules

Issue	Description
SF-1169066 ACM-87411	Provisioning Termination and Attribute Sync rules incorrectly processed local user mapping for pending accounts.
SF-1147687 ACM-87267	Renaming a Notification Rule left an orphaned item in the scheduled tasks for that rule.
SF-1208949 ACM-90043	Detected violations did not associate with remediation workflow jobs during rule processing due to an Oracle buffer overflow error.

Server Core

Issue	Description
SF-1061884 SF-1197693 ACM-83205	Scheduled and manually initiated tasks required improved handling and diagnostics.

User Interface

Issue	Description
SF-954920 ACM-87252	Different security context configurations in the same .csv file did not work as expected.
SF-1073714 ACM-81669	After changing the name of a business unit, the user interface showed the old business unit name when grouping users by business unit.
SF-913568	The User Change data table still showed the User ID field when not selected as a

Issue	Description
ACM-75393	displayed column in Table Options.
SF-612632 ACM-51311	The What Access tab did not disable the filter to show pending entitlements when switching to another application.
SF-947231 ACM-75230	Disabled accounts on the Submit Request > Available Accounts page were not crossed out.

Release 7.1 Patch 3

Information about the 7.1 Patch 3 release is included in the following sections:

What's New in Release 7.1 Patch 3

Note: Custom Workflow Tasks are a reserved capability that should only be enabled for production operations if approved by RSA product support and engineering teams. A warning message will be displayed when enabled.

User Interface Changes in Release 7.1 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
Access Certification ACM-88680	The "Save Tab in Table" option has been removed from table pop-ups.
Access Certification ACM-88254	The user interface displays an “in-progress” indicator when general category bulk maintain actions are in progress.
Access Certification ACM-88929	Export operations are now limited to 5,000 records at a time.
Access Requests ACM-79721	Revocation change requests generated by account change requests will maintain the account property type.
Change Requests and Workflows ACM-71049	The default AFX Manual Fulfillment subprocess workflow now includes a job state node to cancel change items when cancelling fulfillment.
Provisioning ACM-88777	The Workflow ValidReplyAnswers macro now populates and lists URLs in a consistent order.
Request Forms ACM-70736	User filters containing avform.user variables are not replaced with substitute values in the Compare Users field of the Provisioning form.
Security ACM-73739	Enhanced security for page access in RSA Identity Governance and Lifecycle.
User Interface ACM-81449	The Other type for owners is now usable in simple and advanced views.

Fixed Issues in 7.1 Patch 3

The following issues were fixed in RSA Identity Governance and Lifecycle version 7.1 Patch 3.

Access Certification

Issue	Description
SF-1083271 SF-1176983 ACM-83163	After uploading a coverage file to delegate a sign-off to another user, duplicate Entitlements appeared in a User Access Review.
SF-1144992 ACM-85868	An on-hold role review that was closed without changes incorrectly marked a role as "changed".
SF-924608 ACM-72958	Group review results for monitors incorrectly displayed the member count for all groups as zero.
SF-1184310 ACM-88254	After performing bulk maintain actions on general category items, the user interface did not indicate that any action was in process. This caused the user to attempt to perform the action multiple times, even though it was already in progress.
SF-1195963 ACM-88680	A reviewer without required privileges could download the full list of users and attributes from any User Picker pop-up.
SF-1202327 ACM-89970	Large-scale reviews used all available memory and crashed the server with OutOfMemory errors.
SF-1202327 ACM-88929	Out of Memory errors occurred during large reviews.

Access Requests

Issue	Description
SF-1049128 ACM-79721	A change in property types, caused by change requests for accounts that generated revocation change requests for users, led to incomplete information for revocation that failed on fulfillment errors.
SF-1122086 ACM-84828	An automatically generated revocation request would fail when using a directory for an account.
SF-1189389 SF-1189398 SF-1189510 SF-1189404 ACM-88467 ACM-88468 ACM-88485 ACM-88477	The system did not generate change requests from violation remediation actions for revoked accounts when simultaneously revoking and giving exceptional access for multiple accounts that belonged to the same app role.
SF-1223556 ACM-90304	When reverting a pending account, an Oracle error "ORA-19279" prevented successful completion of the action. Also, restarting RSA Identity Governance and Lifecycle while some change requests were not finalized could result in the same Oracle error "ORA-19279" and prevent server initialization that resulted in users not being able to log in.

Account Management

Issue	Description
SF-1143132 ACM-85968	A pending account cancelled in the fulfillment phase still created an account if the name matched to a previously deleted account.
SF-1085269 ACM-83004	An account template for role and rule changes could be improperly mapped to a request form through a workaround.

AFX

Issue	Description
SF-1102654 SF-1131206 SF-1183455 SF-1193888 ACM-85871	AFX enters "not running" status and connectors enters "stopped" status due to locks on the t_av_afx_server_agent table.
SF-1194056 ACM-88781	The maximum length of the JDBC URL field was too short for AFX connectors.
SF-1064046 SF-1120246 ACM-84535	The Oracle Directory Server connector failed to create an account when the userPassword attribute was required for account creation.

Aveksa Statistics Report

Issue	Description
SF-1165448 SF-1170461 ACM-86990 ACM-90517	The ASR did not pull data for Web Application Machine Information.

Change Requests and Workflows

Issue	Description
SF-1043713 SF-1148983 ACM-79531	Workflow variables containing multiple rows of data displayed with the comma delimiters.
SF-1192752 ACM-88582	Change request variables did not appear when fulfillment workflow edits updated the wrong variable.
SF-889452 ACM-71049	The default AFX manual fulfillment subprocess did not have a job state node to cancel change items, which caused change items in a canceled fulfillment to be stuck in "pending verification" status.
SF-981459 ACM-75938	Accounts and entitlements added through the "Complete Manual Activity Before Collection" feature would not appear in the user interface when referenced outside of the Users page.
SF-1058844 ACM-83640	The **Show Job Level Variables** checkbox did not appear for Escalation workflows.

Collector

Issue	Description
SF-1164164 SF-1172536 ACM-86975	Multi-app collectors slowed down when older data was not removed as expected and instead accumulated with each run.

Connector

Issue	Description
SF-1162980 ACM-87472	Active Directory attribute synchronization was unsuccessful in some environments when the account attribute values were set to null.
SF-1059478 ACM-80536	The SAP connector did not support the USERTYP account attribute.

Data Collection Processing and Management

Issue	Description
SF-1166339 ACM-88505	After the ADC ran, the Foreign Security Principal (FSP) membership changes in Active Directory did not update in RSA Identity Governance and Lifecycle.
SF-1165478 ACM-87066	Unification sometimes terminated users and duplicated them into new User IDs.
SF-981459 ACM-75980	Accounts and entitlements added through the "Complete Manual Activity Before Collection" feature were not reconciled or removed after running collection.
SF-1176684 ACM-87842	Performance issues occurred for indirect relationship processing when processing deleted role relationships.

Database Management/Performance

Issue	Description
SF-1150006 ACM-86789	The GATHER_DATABASE_STATISTICS task failed on a buffer overflow error.
SF-1164598 ACM-88699	Illegal TXN State errors were reported in the user interface after applying a patch.

Installer

Issue	Description
SF-1182857 ACM-88297	Schema patching errors occurred when upgrading a WebSphere installation.

Provisioning

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

Reports

Issue	Description
SF-949068 ACM-76876	Reports exported into the CSV or XLS format occasionally did not retain any data.

Request Forms

Issue	Description
SF-1168573 ACM-87946	The password generator URI field did not resolve form variables.
SF-1151669 ACM-86387	A warning message on change requests needed clarification.
SF-1184989 SF-1179125 ACM-88383 ACM-88439	After changing the value of an avform variable, related form controls with display conditions did not update.
SF-887157 SF-957895 SF-1002780 ACM-70736	User filters with avform.user variables added to the Compare Users field of the Provisioning form removed all users instead.
SF-960379 ACM-74603	Form text fields with a long entry did not show the complete text in request or approval screens.
SF-1210320 ACM-89468	When Multiple Account Resolution is set to "per business source" and the request form adds entitlements from multiple applications that are tied to the same underlying directory, account prompts appear for each application instead of once for the directory.
SF-1188323 ACM-88507	When the User Selection screen for an Access Request form has a grouping that contains more than 100,000 users, the following error occurred when expanding and collapsing the grouping: "Error - java.land.IndexOutOfBoundsException: Index: 100000, Size: 100000".

Role Management

Issue	Description
SF-1067111 ACM-66489	When a change request removed a child technical role from a parent business role, it also erroneously removed group entitlements that were shared from a different child technical role with common entitlements.
SF-1113010 ACM-84589	The displayed number of suggestions and violations did not correctly update collection when membership rules changed for a role and the role moved to the pending state.
SF-1089845 ACM-85357	The Role analytics table for missing required entitlements incorrectly showed technical roles as global roles.

Rules

Issue	Description
SF-1139602 ACM-85892	After modifying a collector, a UCD rule detected changes that had already been validated following a previous detection.

Security

Issue	Description
SF-940772 SF-1174388 ACM-73739	Users could access pages in RSA Identity Governance and Lifecycle without required privileges.

User Interface

Issue	Description
SF-1065497 ACM-81449	An invalid identifier error in request forms appeared when using the Other type for owners in a business source filter.
SF-1152397 ACM-86298	Clicking the Back button in the web browser did not load the previous page.

Release 7.1 Patch 2

Information about the 7.1 Patch 2 release is included in the following sections:

What's New in Release 7.1 Patch 2

The following sections describe improvements in version 7.1 Patch 2.

Feature	What's New
Request Forms	The way in which request forms for applications prompt for account information from end users has been improved. Users with only one account are not prompted to select an account. Users with multiple accounts are prompted to select an account as the first step, before the rest of the form is displayed. All aspects of the displayed application request form take the selected account into consideration, eliminating the need to select an account after selecting entitlements.
Connectors	Introduced IBM Security Identity Manager 6.0 connector template for provisioning requests on ISIM.

Deprecated Items in 7.1 Patch 2

Feature	Description
Password Management	As of RSA Identity Governance and Lifecycle 7.1, 32-bit installation of the AD Password Capture tool has been deprecated.

User Interface Changes in Release 7.1 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
Access Certification ACM-87169	The new reviewer interface no longer includes access for terminated users as a low-risk category.
Account Management ACM-83939	When a pending account cannot be renamed due to conflicts, the error is logged in the aveksaServer.log file and the Approval screen does not proceed. The Reject option

Issue	Description
	on the Approval screen shows the tip "Parameter changes other than comments are ignored."
Data Collection Processing and Management ACM-74626	The Application Metadata Collector will only update application business source objects.
Request Forms ACM-64863	The Request Forms wizard disables the Next button until all form elements on a page are loaded.
Request Forms ACM-77882	Drop-down, Multi-select, and Number fields can be populated by avform attribute selectors used as the default value.
Request Forms ACM-83637	The JavaScript block form control no longer allows Display conditions. The Display tab for this form control displays a message for the restriction. When Enable conditions are set, the JavaScript block entered is executed only when the conditions are satisfied. If there are no conditions set, then the JavaScript block is executed whenever the form runs.
Request Forms ACM-88604	Multiple account resolution can be configured on a request form to prompt for every change or per business source.

Fixed Issues in 7.1 Patch 2

The following issues were fixed in RSA Identity Governance and Lifecycle version 7.1 Patch 2.

Access Certification

Issue	Description
SF-1124917 ACM-84693	A null pointer exception occurred when a reviewer opened the review using the email link, performed an action, then saved.
SF-1153118 ACM-86633	Revoking a user during a fine-grained role review resulted in a long delay before the status bar was updated.
SF-1110632 ACM-84590	Application coverage statistics showed incorrect values by not including roles and groups.
SF-1058478 ACM-82186	Triggering the Escalation Workflow of Review Reassign sent two emails to the user.
SF-1184310 ACM-88254	After performing bulk maintain actions on general category items, the user interface did not indicate that any action was in process. This caused the user to attempt to perform the action multiple times, even though it was already in progress.
SF-1167341 ACM-87169	The new reviewer interface included access for terminated users in the low-risk category by default.

Access Requests

Issue	Description
SF-1081182 ACM-83561	Change requests could be skipped by the processing workflow.

Account Management

Issue	Description
SF-1109146 ACM-83939	If the names of created or pending accounts were changed during fulfillment, duplicate accounts formed for returning users with deleted accounts.

AFX

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

Application Wizards

Issue	Description
SF-1142271 ACM-85633	Two or more users with the same name and different user IDs could not be added to a business unit's Other Business Owner field.

Authentication

Issue	Description
SF-856151 ACM-65647	Accessing an approval URL when logged in through SSO caused a NullPointerException error.
SF-1059226 ACM-84670	The Forgot Password feature did not work after a change in the user locale by the browser language settings.

Change Requests and Workflows

Issue	Description
SF-929278 SF-1042033 SF-1063111 ACM-73194	The Provisioning Command node did not save attribute values correctly when commas were used.
SF-1138470 SF-1125576 ACM-86190	Imported workflows could not send email after an upgrade because of email body errors and Send Email node errors.

Issue	Description
ACM-85810	
SF-1077035 SF-1146372 ACM-83585	Approval or Fulfillment nodes sometimes skipped when retrying after a concurrency error did not update the job with new node and sub-process data.
SF-1156274 ACM-86559	The workflow reference ID appeared for a subprocess instead of the workflow name when "Only show workflows similar to the current workflow" was checked.
SF-1045572 ACM-79675	The provisioning node mapping misaligned nodes when mapping a hardcoded value to a parameter value with a comma.
SF-1176466 SF-1181417 ACM-88269	AFX Requests with the "Entitlements Require Account" setting enabled would stall in the "Waiting for Dependencies" state.
SF-1083779 ACM-82500	Change requests with Joiner rules could experience a deadlock error caused by a Workpoint bug when the workflow is under a heavy load.
SF-1152348 ACM-86911	When a Workpoint license check failed due to a connection issue, the user was required to restart the system or reload the license.
SF-1127411 ACM-86163	The workflow business calendar did not consider holiday hours when assigning due dates to workflow actions.

Collector

Issue	Description
SF-844956 SF-1087717 ACM-67283	Referrals were not ignored when "Ignore Referral" was checked in the connection settings.
SF-833758 SF-894036 ACM-66892	When an IDC collected the accountExpires date attribute from an Active Directory source, the time value varied on every collection based on the time zone.

Connector

Issue	Description
SF-1136239 ACM-85602	The Generic Database template with db2 type selected resulted in an error.
SF-894746 ACM-71014	The Active Directory AFX Connector could not set the PASSWD_CANT_CHANGE Active Directory attribute.

Dashboard

Issue	Description
SF-1167801 ACM-87247	A custom user link in a dashboard appended "&width=null&height=null" to the URL, which caused some external pages to not load properly.

Data Collection Processing and Management

Issue	Description
SF-1131077 ACM-85203	A sub-group to group membership was rejected because the name of the group had a space at the end that was not consistently trimmed at the source and when collected.
ACM-85608	Calculated totals for applications did not include group memberships as entitlements.
SF-1145208 ACM-86417	Role collectors aborted runs for groups that were role entitlements because of a case-insensitive search.
SF-1159109 ACM-86620	The DAG collector queries took many hours longer than expected to complete.
SF-1120976 ACM-86422	Collected subgroups from an LDAP were resolved as accounts instead of as groups.
SF-942302 ACM-74626	The Application Metadata Collector updated some non-application business source objects, such as role sets, in error.
SF-1160713 ACM-87431	User type attributes did not consistently appear for a unified user after a unification.

Database Management/Performance

Issue	Description
SF-1164598 ACM-86987	The database slowed, reported multiple errors, and then used up all resources when conducting bulk reviews on thousands of items.

Email

Issue	Description
SF-1136705 ACM-85359	Escalation emails were not updating the value used by the runtime to send with proper priority.
SF-1004034 ACM-80529	A Review Reminder email configured for 24-hour intervals generated at 12-hour intervals instead.
SF-1162253 ACM-86909	Security access request approval email links did not work.

Installer

Issue	Description
SF-1141841 ACM-86014	A supported database version could not be confirmed during migration.
SF-1163231 SF-1166981 ACM-87107	The generateLoginKey.sh script reported a missing command error when used.

Metadata Import/Export

Issue	Description
ACM-84989	Metadata sometimes exported with random, duplicated objects on subsequent attempts after the first export.

Request Forms

Issue	Description
SF-1112926 ACM-85657	Out-of-the-box Application Business Source attributes returned null values when called through variables in request forms.
SF-1143371 ACM-85654	The text area field was not validated for the maximum character limit if the related question had an apostrophe.
SF-1010220 ACM-77882	Drop-down, Multi-Select and Number fields did not populate if the avform attribute selectors were used as the default value.
SF-1109812 ACM-83706	The Drop Down Select control type for request forms was not disabled as intended if Enable conditions were set.
SF-1094196 ACM-83637	In request forms, the Display and Enable conditions for the Javascript field in request forms did not work as expected.
SF-968958 ACM-76010	The "Allow Multiple Selections" setting did not work correctly in a User Account Table field in a form.
SF-1100787 ACM-84628	Custom dropdowns did not retain selections with web service fields.
SF-1127904 ACM-85244	A request form did not handle user details containing "\" properly for user pickers and the provisioning command.
SF-840034 SF-999420 ACM-67318	A request form did not show the correct entry when an apostrophe is present in the value of a variable.
SF-1097313 ACM-83168	The selected value for a radio button appeared as ??? when passed to other form controls through the avform variable.
SF-815680 ACM-64863	Request forms allowed users to move to the next page before all the form fields had finished loading.
SF-1131084 ACM-85886	Child entitlements of pre-selected entitlements did not load in an entitlement table form control.
SF-1889550 ACM-88604	Multiple account resolution prompts for every entitlement change created as account changes could lead to excessive prompts.

Role Management

Issue	Description
SF-22039 ACM-48746	The Request Hierarchy Children entitlement selector allowed selected entitlements to exceed the actual total.

Issue	Description
SF-1071138 ACM-74902	The error "Unable to find RoleSet ID" appeared in logs while creating a role collector with the raw name and alt name roleset attributes as different entries.
SF-1190065 ACM-88496	The user interface did not display a role in a role set due to a query error.

Rules

Issue	Description
SF-1121216 ACM-84791	A condition for access containing IN for a rules definition could not be re-edited for attributes with case-insensitive "name" in the label.
SF-774383 ACM-63346	After migration, violations appeared with the wrong state.

User Interface

Issue	Description
SF-768669 ACM-65157	A truncated file size limit error was displayed for the attachments control type when using Internet Explorer.
SF-830319 ACM-66283	The Owner attribute did not appear in the table options of the What Access tab under Resources.
SF-1126909 SF-1185935 ACM-85023	Pressing Enter on the Forgot Password screen canceled the process.
SF-19207 SF-684770 ACM-45115	The date in the European format of DD/MM/YYYY did not properly appear for the English (UK) locale.
SF-904694 SF-873589 SF-1156305 ACM-72163	Benign errors appeared when a web service authenticated the AveksaAdmin user when no Aveksa system authentication source was defined for AveksaAdmin.

Release 7.1 Patch 1

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

What's New in Release 7.1 Patch 1

Feature	What's New
AFX	The AFX connector has improved performance when mapping unused variables in large environments.
Change Requests and Workflow	Fulfillment workflows now include a technical approval node. The technical approval node prompts the technical owner to approve a change request before fulfillment.

User Interface Changes in Release 7.1 Patch 1

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

Issue	Description
Access Certification ACM-68187	The Bulk Actions dialog box displays all supported actions as a drop down field and includes **Add Comment** as a separate bulk action. **Maintain with Expiration** is also listed as a separate bulk action when a selected expiration date field is displayed and mandatory.
Account Management ACM-78326	Additional account parameters from an account template will now display in the Account info pop-up.
Change Requests and Workflow ACM-84016	The provisioning command node properties do not display job variables tied to data that it cannot directly access.
Change Requests and Workflow ACM-84218 ACM-84554	User access requests for entitlement changes apply the following rules: • User entitlement changes that require accounts are always account changes. • User entitlement changes with no assigned accounts remain user changes. • User entitlement changes with one assigned account are created as account changes. • User entitlement changes with multiple assigned accounts prompt for account selection and are created as account changes.
Change Requests and Workflow	The number of work items retained in the workflow history is now limited to reduce the amount of data loaded.

Issue	Description
ACM-80901	
Collector ACM-75432	The attribute "lastlogontimestamp", always collected as a date-type value, can be stored in a custom attribute of either string-type integer value or a date-type value. A string-type integer value is automatically converted to the date-type value formatted as “yyyy-MM-dd HH:mm:ss”.
Data Collection Processing and Management ACM-82998	The IDC User Interface now shows the "Requires Full Refresh" status like the other collectors.
Email ACM-79253	Generated emails of exported reports attach the report file with a lowercase extension.
Email ACM-83216	Email reply processing looks for the dynamically assigned individual in roles defined as a dynamic resource or group.
Password Management ACM-81479	The Default External Reset Password Form is available. It can be customized to have external validation URI to apply consistent validation. External reset password pages display as a full page. Users cannot continue to the next page unless the external reset password page meets the conditions for validation.
Reports ACM-67195	Reports exported to an Excel spreadsheet now use the .xlsx extension.
Reports ACM-81849	If invalid characters are detected the report file name, the detected characters are replaced with an underscore. Strings of invalid characters are replaced with a single underscore. The user interface allows characters not valid for the file name.
Request Forms ACM-65018	Non-visual tables for accounts and entitlements will not display on a submitted request form.
Role Management ACM-65297	The entitlement type now displays in brackets next to the entitlement display name when setting an entitlement rule in a role set.
Role Management ACM-75430	The Role Import process warns that collected roles, if imported, will be converted into local roles.
Role Management ACM-81602	Coarse-grained role reviews no longer include a Remove button or allow edits for entitlements and members.
Rules ACM-84810	The form for the Violation Remediation workflow node does not show out-of-the-box form controls that will not work for the node.
Security ACM-84155	Users now require at least view permissions to see the properties of a workflow. Edit permissions are required for users to edit a workflow. These permissions also apply to parent or child jobs of a workflow. The Workflow tab for an approval or fulfillment request will only display the workflow image.
User Interface ACM-77791	The Max Users Per Change Request setting in Access Configuration displays as "--" on the Settings tab if not assigned a value.
Web Services	Web service requests to add an account to a group now associate users that are

Issue	Description
ACM-81967	mapped to the account. A web service change request involving access for multiple users for a shared account now displays "Multiple Users" instead of a single user in the AccountChanges table. A user's shared account displays changes raised by other mapped users in their Requests tab.

Fixed Issues in 7.1 Patch 1

The following issues were fixed in RSA Identity Governance and Lifecycle version 7.1 Patch 1.

Access Certification

Issue	Description
SF-1044154 SF-1027351 ACM-82969	Change Requests in Open status without a workflow ID defaulted to the Explicit Access workflow after restarting the application.
SF-839034 ACM-66789	A review opened through an email link, then canceled, opened a null page after confirmation instead of the home page.
SF-855955 ACM-68187	Comments for review items could not be applied as part of a bulk update.
SF-1120715 ACM-84607	The email link to view a role review opened to an error page.
SF-1008666 SF-1027715 ACM-79783	Non-existent access to a group appeared for users in a User Access Review.
SF-597513 ACM-51149	Multiple Account Review attributes did not properly translate to other languages.

Access Requests

Issue	Description
SF-964684 ACM-76816	Access Requests with violations could be submitted by requestors when the filter was defined with more than one role attribute.
SF-1021090 ACM-78198	Approval nodes assigned access requests to out-of-office supervisors if those supervisors were part of the approval workflow at another level.
SF-1102047 ACM-83563	Custom attribute value lists degraded the performance of rendering the User Access pages.
SF-01110863 ACM-84248	Attributes with “on” and no date caused an exception error during the display of the milestone on the Change Request Detail page.
SF-1066622 ACM-83225	An error occurred identifying the application name in a change request when the application had a Directory For Accounts setting.
SF-1122693	A pending change request with a large number of new accounts could cause a cleanup issue when restarting.

Issue	Description
ACM-84601	
SF-1098397 ACM-83297	A Review query was not optimized for large datasets and used too much database memory.
SF-818651 ACM-64918	Business Sources excluded from Add Access and Suggestions were visible under Requests > Create Requests > Add Access, but their entitlements could not be requested.
SF-1042229 SF-1122224 ACM-80274	The manual activity assignment link became disabled after a few hours if dynamic groups or roles were in use.
SF-1103472 ACM-84436	AFX logs were not filtered as relevant to a request.
SF-1133285 ACM-85099	When a web service was assigned for a request, an error occurred when clicking on the default form under "Additional Information".

Account Management

Issue	Description
SF-837790 SF-694892 SF-828508 SF-1044336 ACM-78326	An account template configured with additional account parameters failed to add those parameters to a created account.
SF-1104583 ACM-84929	Imported mapping that had been deleted and recollected from the account data collector source would create duplicate mapping.

Application Wizards

Issue	Description
SF-839184 ACM-67710	The Users count under Applications > General did not update after importing or updating the mapping.

Change Requests and Workflows

Issue	Description
SF-1053443 ACM-83569	If Enable Email Reply Processing was unchecked and saved, then related options were not properly hidden.
SF-1101627 ACM-83545	A Delete Account change request could be marked as complete but still show a status of "Pending Action".
SF-1069608 ACM-81876	Manual Request Additional Info escalations could prevent an automatic Reassign to Supervisor escalation from running as expected.
SF-1104201 ACM-83552	The save button did not function properly when a resource, escalation, job variable, or webservice response was added, edited, or deleted.
SF-1022154	A Change request generated using an unowned group and an owned group would

Issue	Description
ACM-78550	incorrectly assign all of the change request items to the second group's owner for approval.
SF-4036115 ACM-82463	When generating a change request with users who had outstanding change requests, the generated change request incorrectly excluded any users who did not have an outstanding change request.
SF-1098925 ACM-83236	Imported legacy workflows created before version 7.0.1 had a legacy value not handled by the new architect editor.
SF-1110903 ACM-84016	The Provisioning Command node did not display job variables in the node properties.
SF-1118999 SF-1119764 ACM-84554 ACM-84218	A user access request with multiple entitlement changes did not reliably create account change items for adding entitlements depending on the order of selected actions.
SF-1143477 ACM-85731	After an upgrade, transition were not displayed in processing workflows that were created in the previous product version.
SF-684868 ACM-55740	After completing an activity, users could see all completed activity on the By Entitlement tab instead of just their own.
SF-1077691 ACM-81947	An exception error occurred when evaluating fulfillments with dynamic roles and group resources.
SF-1040676 ACM-79305	An entire change request would be rejected at the fulfillment phase if it had an entitlement deleted by a partial rejection in the approval phase.
SF-867542 ACM-74045	Activity nodes in a workflow were skipped if AFX fulfillment came back as Completed.
SF-1116690 ACM-85129	SOAP and REST web service nodes could not be exited if the code window was expanded.

Collector

Issue	Description
SF-1110276 ACM-83742	Collection failed when the internal data file was larger than 2.15 gigabytes.
SF-953019 SF-1094710 ACM-74103	A line break character in search filters caused the test collection to fail for the LDAP collector.
SF-964259 ACM-75432	A custom string attribute used for collection did not collect the LastLogonTimestamp attribute as expected.
SF-1039961 SF-1112908 ACM-84256	The Salesforce collector did not collect LastLoginDate as expected due to an invalid date format error.

Connector

Issue	Description
SF-1111150 ACM-84090	After an upgrade, attribute synchronization on the AD connector applied the attribute_sync prefix to non-empty & non-account variables, which updated values not required as well.
SF-976731 ACM-79126	Account template parameters did not correctly expand variables in password type attribute fields.

Dashboard

Issue	Description
SF-1032894 ACM-80335	Dashboard links containing a query parameter that included a bind variable did not return the expected results.

Data Collection Processing and Management

Issue	Description
SF-1088219 ACM-82998	The IDC User Interface did not show whether the IDC required a Full Refresh.
SF-1104583 ACM-83603	Pending User Account mapping and subsequent local mapping were removed every time the ADC ran collection.
SF-1100515 ACM-83254	A collection that failed on the circuit breaker update did not remove the green check mark from the Last Successful Collection Date field.
SF-1063378 ACM-82700	After unmapping users from the accounts, the users sometimes erroneously retained access.
SF-1100498 ACM-83252	Procedures to purge older raw datasets caused circuit breaker failures when they erroneously purged raw datasets for collectors queued for processing.
ACM-53235	Internal data files such as STX tables and temporary data files in the server/default/deploy/aveksa.ear/aveksa.war/WEB-INF/AveksaDataDir directory were not removed as expected if the "Remove Internal Data Files After Upload" option was set to Yes.
SF-1068551 SF-930028 ACM-83338 ACM-73635	For users making role changes, role data collection would sometimes cause deadlocks due to database-stored procedures making unnecessary row updates to roles, even when they were not changed.
SF-596501 SF-714442 SF-820106 ACM-50485	Collection fails with an unclear error message when the collection source contains a special character that cannot be parsed.
SF-1115169 ACM-84129	Starting a unification run with migrated user records from before 7.x failed with "ORA-30926: unable to get a stable set of rows in the source tables" in 7.0.2 p2.
SF-1121551 SF-1128128	Unifying data with duplicate values caused failed collections with the message "ORA-30926: unable to get a stable set of rows in the source tables".

Issue	Description
ACM-84547 ACM-84928	
SF-1103183 ACM-84750	The "Who Has Access" tab for Data Resources was not populated after a long-running data collection by the primary DAC that was misidentified as secondary.
SF-1059311 ACM-83235	The DAG collector stalled after pre-processing a large data validation query.
SF-988361 ACM-83488	The account and entitlement data collectors did not collect user attributes CAS6 through CAS10 for indirect group entitlements.
SF-1133387 ACM-85100	The account and entitlement data collectors did not collect CAS user attributes in the correct order and could not properly assign the value of CAS10 as a result.
SF-1101593 ACM-83516	Unifications could fail due to improper clean-up of the tables used for prior data collections.
SF-1131773 ACM-85098	Unification sometimes assigned a deletion date for users that prevented them from logging in.
SF-1097757 SF-1119006 SF-1042848 SF-1042140 SF-1114071 SF-1126989 SF-1077894 ACM-85534	Temporary STX tables were left behind if the circuit breaker was triggered.
ACM-85488	User access to data resources could not be reviewed if assigned only through a group that was not properly tagged after data collection.
SF-1058100 ACM-80563	When a user was moved from one IDC to another, unification terminated the original user and created a duplicate user.

Database Management/Performance

Issue	Description
SF-01123301 ACM-84609	Data archiving had a processing failure.
SF-1164598 ACM-86987	The database slowed, reported multiple errors, and then used up all resources when conducting bulk reviews on thousands of items.

Email

Issue	Description
SF-1067879 SF-1069696 SF-1134843	If the special character % was in the e-mail content, then the email could not be generated.

Issue	Description
ACM-81341	
SF-1039470 ACM-79253	Emails generated for exported reports incorrectly capitalized the report file extension.
SF-1101300 ACM-83537	Reports exported to an Excel spreadsheet did not restore a previously deleted temporary folder and, as a result, returned blank rows instead of the expected data.
SF-1086751 ACM-83216	Email processing failed and displayed the error "Wrong user replied" for approvals sent to dynamically assigned approvers in a role.

Installer

Issue	Description
SF-970037 SF-1108073 ACM-76001	Aveksa.ear contained duplicate files that caused zip errors during deployment.
SF-1137353 SF-1142351 SF-1138013 ACM-85438	The installer checked for unneeded packages and caused installation in a WildFly environment to fail.
SF-1115317 ACM-84107	A typo appeared in the installOracle.sh script.
SF-1129043 SF-1139113 SF-1136656 ACM-85437	Installation or upgrade on Red Hat 6.5 and 6.8 failed when IPv6 was disabled.
SF-942673 ACM-73935	The installation or upgrade process would get stuck when one or more required install packages were missing.
SF-1130896 SF-1139955 SF-1150455 ACM-85021	The aveksaWFArchitect.ear file could not be deployed on WebLogic 12.2.1.3.0 due to a conflict in the Java Spring-Boot library.
SF-1150455 SF-1176964 ACM-86894	A schema could not be created or migrated when using non-default tablespace names.

Password Management

Issue	Description
SF-924320 ACM-73375	The View Password URL could not be correctly configured through the User Interface.
SF-1069908 ACM-81479	Password validation did not work consistently from the user interface and from an external password reset link.

Reports

Issue	Description
SF-1043556 ACM-81849	The / character in a report file name created a report schedule that failed if the option to send attachments was enabled.
SF-1004352 ACM-79058	A new chart could not be created with the same name as an existing tabular report.
SF-826817 ACM-67195	Reports exported using the .xls file extension were not properly formatted.
SF-767212 SF-824328 ACM-60522	After upgrading, reports containing Cyrillic characters still did not display correctly when exported as .xls or .csv filetypes.
SF-838887 ACM-71716	The report template "Entitlement Review Item Details by Reviewer" did not display the custom review state.
SF-01143644 ACM-85658	The order of the list columns available in the Report Column tab changed randomly.
SF-647482 ACM-52763	Imported Custom Report templates copied unnecessary attributes that caused errors.

Request Forms

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

Issue	Description
SF-1086944 ACM-83740	Multiple entitlement tables that used Display conditions, Enable conditions, and Form variables in their entitlement rules sometimes displayed improperly.

Role Management

Issue	Description
SF-1069369 ACM-81602	The user interface for coarse-grained role reviews provided options to remove or edit members and entitlements, even though coarse-grained role reviews are intended for high-level review and not to make individual changes.
SF-817316 SF-844023 ACM-65297	Custom attributes created with the same name but assigned to different entitlement types appeared identical and did not work correctly when setting an entitlement rule in a role set.
SF-1112926 ACM-85657	Out-of-the-box Application Business Source attributes returned null values when called through variables in request forms.
SF-1149895 SF-1083679 SF-1123786 ACM-86112 ACM-83273	Fixes to the role set persistence of a role caused problems with entitlements when there were role set changes.
SF-1142958 ACM-85634	A Null pointer exception error occurred when creating a new role while logged in as the business role owner of a role set.
SF-1089845 SF-1132001 ACM-84396	Cascaded roles were missing to be added as entitlements while creating a change request from the Role Missing Entitlements rule execution.
SF-1078256 ACM-82957	After importing a modified XML file of existing global roles, the Long Description was not updated.
SF-839546 ACM-66820	A new role with no members or entitlements did not appear in search results when the search filter was set with the member or entitlement count as zero.
SF-963152 ACM-63734 ACM-75430	Collected roles that were exported did not fully import when imported into same environment.

Rules

Issue	Description
SF-1052613 ACM-84945	When the Attribute Change rule for Managed Attributes used the "Set to old value of" argument, the rule sometimes failed to set values after the first user matched by the rule.
SF-1120488 ACM-84536	During access request creation, when a user views the Accounts selection screen and then goes back to the previous screens to make changes, violations by the new changes were sometimes not displayed.
SF-1127651 ACM-84810	Out-of-the-box workflow form controls were listed in the Violation Remediation node that did not work for the node.

Issue	Description
SF-1114903 ACM-83574	Changing the User Access/Separation of Duty Rule definition closed some violations but left their remediation workflows active.
ACM-83212	New violations could incorrectly be added to existing remediation workflows, when a new workflow was necessary.
SF-1105975 ACM-83937	The number of violations did not appear correctly in the status column.
SF-1057748 SF-1125122 ACM-84105	The user interface did not display violations that were not in sync with the remediation workflow to remediators.
SF-1125118 ACM-84592	A rule violation remained in Pending Revocation status after rejection of a corresponding change request item.
SF-1101217 ACM-83760	An Out of Memory error occurred while processing a large number of Role Membership Rule Difference rules.
SF-1095861 ACM-83120	When a change request was created by a role change, decision Nodes ignored the "Contains at least one violation" condition.
SF-1025263 SF-1026091 SF-1073300 SF-1126913 ACM-78589	Change requests created by an unauthorized change detection rule identified the wrong user in the details.

Security

Issue	Description
SF-1095483 ACM-84155	Applied security fixes for workflow editor properties.

Server Core

Issue	Description
SF-903632 ACM-71675	A domain controller node in a hardware appliance with a local database could not stop, start, restart, or status-check the database using the aveksa_cluster script.

User Interface

Issue	Description
SF-596472 ACM-51112	When editing review definitions, the Allow Expiration and Comments are Required checkboxes were cleared if the user switched tabs.
SF-843449 SF-931419 SF-932453 ACM-67243	Logging out led to a blank screen if confirmations for logging out were disabled.
SF-791436	After adjusting table options, some columns did not display as configured when

Issue	Description
ACM-62724	switching from a Group review result to a User review result.
SF-1001038 ACM-77791	The Max Users Per Change Request setting in Access Configuration disappeared from the Settings tab if not assigned a value.
SF-1086944 ACM-85029	Performance issues occurred on the General tab of a role set after applying entitlement and membership rules.
SF-884453 SF-884449 SF-936962 SF-982809 SF-1084195 ACM-73706	Heartbeats, which help to avoid server timeouts when using forms and the Architect workflow editor, generated benign errors in the server log.
SF-1127021 SF-1149655 SF-1152703 SF-1149987 ACM-85554	Changes in the customerstrings.properties file were not saved after an application server restart.
SF-620510 ACM-52883	Underscores and spaces incorrectly replaced Hebrew characters in the user interface.
SF-1110294 ACM-85141	The unique_ID attribute was not displayed on the summary page after changing the language under user options.
SF-1104724 ACM-84228	Extended user attributes were not displayed on the summary page after changing the language under user options.
SF-967960 ACM-76184 ACM-76185	Attributes did not display when searching in the Business Units or Application list.

Web Services

Issue	Description
SF-1035349 ACM-81967	Web service requests did not show affected users.

Known Issues and Limitations

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

Tracking ID	Description
ACM-87806	The AFX server may not start after an upgrade. **Workaround**: 1. Download the server keystore file in **Admin > System > Security > Server Certificate Store for Agent SSL Connections**.

Tracking ID	Description
	2. Copy the server keystore file to /home/oracle/keystore. Overwrite or delete the existing file. 3. Download the client keystore for the AFX server in **AFX > Servers > Download Keystore**. 4. Copy the client keystore file to /home/oracle/AFX/esb/conf. Overwrite or delete the existing file. 5. Restart the servers for both AFX and RSA Identity Governance and Lifecycle.
ACM-87951	Custom images for the logo, header, favicon, login background, and footer may not be immediately applied to the user interface. **Workaround:** Restart the RSA Identity Governance and Lifecycle server.
ACM-88258	Custom favicon files are not displayed in Internet Explorer 11 and Microsoft Edge due to an HTTPS certificate error.

Release 7.1

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

What's New in Release 7.1

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

Feature Highlights

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

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

Additional Features and Improvements

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.
AFX-Install	File name validation has been added for connectors and connector templates. The following characters are not allowed in file names: \ / : * ? " < > |
Change Requests and Workflows	The following changes have been made to change requests and workflows: • The workflow editor has been updated to Workpoint 4.4.0 Patch 10. • A category attribute has been added for workflow definitions and jobs that support grouping. The category value can be set in the workflow editor.

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

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

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

Deprecated Items in 7.1

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

User Interface Changes in Release 7.1

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

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

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

Issue	Description
Data Collection Processing and Management	The HasData option is no longer supported for new role data collectors. Existing collectors that currently use this option are not affected.
Descriptions	RSA Identity Governance and Lifecycle now requires that business descriptions for groups contain an application scope. When you create a new business description for a group that does not apply to a set, you must select an application with which to associate the business description before you can select the group. When you import business descriptions from an XML file, you must ensure that an application is specified for each business description that applies to a group. When updating or migrating RSA Identity Governance and Lifecycle from a previous version, RSA Identity Governance and Lifecycle deletes group business descriptions that are not actively in use. Before you migrate, run the provided pre-migration queries to identify any group business descriptions that will be deleted by the migration process. If you still need these group business descriptions, you can re-import them with an application reference in the import file, or you can manually recreate them after migration. For more information, see the "Migration Queries for Group Business Descriptions" section in Install a Patch on page 10.
Metadata Import and Export	The User Attributes check box has been removed from the Import/Export dialog. All attributes, including user attributes, can be imported or exported by selecting the Attributes check box.
Reports	Report headers wrap column text to avoid hiding important information.
Request Forms	Support has been added for connecting to a web service using authentication when adding a field to an access request form. When you add a field to an access request form and select the control type "Drop Down select with Web Service", under Options, you can now configure the Authentication Type, Authentication User, and Authentication Password for the connection to the web service.
Request Forms	The Password Reset form can now process all field components that would create a change item.
Role Management	Users editing a role without access to the assigned roleset will see the assigned roleset but will not be able to change it.
Rules	• When remediating an SoD rule violation, you should not be able to alter your original action while the confirmation dialog is open. • Common entitlements are no longer detected in the entitlement coverage of a separation of duties (SoD) rule. As a result, SoD rules are not saved as an invalid rule. The rule detail page no longer displays a message containing the common entitlements between the two entitlement sets. SoD rules that are saved with the Invalid status are migrated to the Inactive status. When you import a rule that has an Invalid status, it is saved with an Inactive status.

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

Fixed Issues in 7.1

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

Access Certification

Issue	Description
SF-803269 SF-927964 SF-979348 ACM-63517 ACM-75730	Specifying date-type attributes for user review criteria resulted in the following error: ORA-01840: input value not long enough for date format.
SF-835743 SF-915044 ACM-66520	The Grouped by Application tab for a user review did not display groups and roles by their directory or role set as expected.
SF-976100 ACM-76116	"Update Un-Reviewed Items" action in review item history showed AveksaAdmin instead of the actual user who performed the action.
SF-817109 ACM-64793	Reviewer delegation or reassignment comments greater than 4,000 characters in length prevented saving a review change with the JDBCException - ORA-01461 error.
SF-831090 ACM-67887	Reviewers with only "save" privileges and not sign-off privileges could not properly see review items queried by V_AVR_ER_ITEM_DETAIL.
SF-1008441 ACM-78070	The accounts and entitlements count displayed incorrect values when a reviewer applied more than one grouping.
SF-1037868 ACM-79267	The review results for user access reviews did not include the role entitlements for all users.
SF-1008019 ACM-78225	Bulk Actions did not apply to accounts with unreviewed entitlements if the accounts were signed off.
SF-1202327 ACM-89970	Large-scale reviews used all available memory and crashed the server with OutOfMemory errors.

Access Requests

Issue	Description
SF-903529 SF-890332 SF-908531 SF-934592 ACM-71833	In a form-based workflow where forms were approved and then fulfilled, the workflow intermittently skipped the approval step.

Issue	Description
ACM-73254	
SF-942388 SF-955309 ACM-73931	Revocation change requests did not display work items.
SF-983142 ACM-75849	Rejecting one user in a request with multiple users during the approval phase removed too many pending accounts.
SF-917409 ACM-72808	Under Requests > Activities > By Entitlement and Requests > Approvals > By Entitlement, the Monitoring Policy view does not display activities for deleted accounts.
SF-823162 ACM-68232	The CSV file exported from Requests > Activities was corrupted.
SF-1025998 ACM-79262	Account removal triggered for a user with "Complete Manual Activity before collection" set to "Yes" did not completely remove accounts from user access before the collection.
SF-909706 ACM-72131	On the By Entitlement tab of the My Activities page, an account's custom attributes were not populated.
SF-959975 ACM-74600	The Fulfillment Handler was using the XML configuration instead of the internal configuration.
SF-898527 SF-1029461 ACM-73205	Manual workflow activity showed an incorrect timestamp when an escalation canceled the workflow.
SF-1063876 ACM-81061	A "Request could not be handled" error occurred when clicking on a submitted form request created via web service.
SF-865253 ACM-70239	The "last reviewed" or "completed on" date collected in a user access review was not displayed in the user access tab.
SF-1121505 ACM-86374	Change Verification was still pending for an Account or group access removal after the account or group was deleted.

Account Management

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

AFX

Issue	Description
SF-1000278	The AFX SOAP Connector used the wrong SOAPAction Header from the WSDL when

Issue	Description
ACM-77008	multiple SOAPActions shared the same SOAP XML request body.
SF-1021681 ACM-79230	ServiceNow documentation needed additional details about permissions.

Authentication

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

Change Requests and Workflows

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

Issue	Description
SF-787423 SF-799534 SF-944220 ACM-67252 ACM-73747 ACM-63718	cause some workflow requests to be stuck in open state, stall on nodes like the Manual Fulfillment Node, or generate an ORA-02291 integrity constraint error.
SF-956207 ACM-75139	In a manual activity workflow, a Mark Verified Node could erroneously complete verification of manual fulfillments.
SF-745588 ACM-60984	The user using the REST Web Services Node was unable to set "Content-Type", which instead defaults to "text/plain".
SF-920455 SF-910312 ACM-73174	When “Wait for Result” was selected, workflows were stuck in the Provisioning Command phase.
SF-895630 ACM-71205	Workflow Java node was unable to save configuration.
SF-845740 ACM-67829	After pending submission change requests were removed by a clean-up task, the pending accounts were deleted but the dependent change request items remained.
SF-913090 ACM-72140	A group entitlement was not included in a change request when added from a role review.
SF-956470 ACM-74461	The workflow job history did not filter out jobs that were being deleted by the purge process, causing an ORA-01722 invalid number error.
SF-936413 SF-993165 ACM-73792 ACM-76475	An error could occur when all line items were rejected in a change request if the system processed the workflow before it could process the line item changes.
ACM-76117	Large workflows usually with more than 23 nodes could not be saved.
SF-974932 ACM-75348	The drop-down list of processes in a child workflow could not show a list of more than 100 processes.
SF-820520 ACM-66029	Duplicate 'remove' change items appeared from a request to remove a role from a user that had duplicated entitlements.
SF-988230 ACM-76091	The REST Web Service node could not use user data to process a response variable.
SF-988600 ACM-76630	The workflow editor would not allow an invalid workflow condition to be displayed on a decision node.
SF-1000082 ACM-76911	Passing null or undefined workflow variables between nodes may have been stopped by a null pointer exception error.
SF-906471 ACM-72817	Importing a workflow with the overwrite option did not update the workflow name.

Issue	Description
SF-997361 ACM-77724	Conversions of decision nodes did not succeed unless performed during a patch upgrade.
SF-1017258 ACM-77999	A subprocess node did not handle the ability to add group and role owner attributes.
SF-1025290 ACM-78311	An unprivileged end user could edit the workflow to approve requests.
SF-990759 SF-994652 ACM-76958	Account data change verification for the Windows Server accounts collector would abort after running for more than 16 hours.
SF-951308 ACM-77144	Non-numeric values in the wp_proci table's lu_id field caused the workflow job table to not display properly.
SF-1021962 ACM-78218	The URL workflow variable didn’t resolve correctly when an escalation was raised on a request workflow.
SF-847108 SF-895584 ACM-61009	Performance optimizations for AFX queries in Oracle 12c.
SF-042252 ACM-79705	A business owner assigned to an application could approve and reject other, unassigned applications kept in the same directory for accounts grouped by business fields.
SF-931653 ACM-73399	In a workflow, a resource could not be modified when a dependent Group, User, or Role could not be found on an imported server.
SF-917117 ACM-72339	In the Workflow Editor, saving SQL nodes with the variable type Public could result in the Oracle error: "ORA-00972: Identifier is too long."
SF-921304 ACM-72337	When configuring a decision node to check whether a workflow variable exists, the Right Operand field is incorrectly required.
SF-991315 ACM-76476	Concurrent processing of a role management database update and change requests risked an indefinite open state for change requests.
SF-999080 ACM-77324	Workflow Editor SQL windows did not resize.
SF-946297 ACM-73893	A user could edit a workflow email node and save changes with the Refresh button without the required privileges for both actions.
SF-965923 ACM-74833	A collector node in the workflow editor did not validate for a selected account data collector.
SF-921304 SF-952404 ACM-72550	The save button did not enable for changing the "Evaluated to true" checkbox on a decision transition unless another change was made to the transition.
SF-1018384 ACM-78740	Exclusion rules for a node did not properly apply to employees designated as a delegate by an out-of-office supervisor.

Issue	Description
ACM-72111	Workflow form compilation errors occurred due to conflicts with ports secured by SSL.
SF-1044220 ACM-80257	A change request did not successfully complete if a business owner's rejection re-mapped the account name derived from the account template to the account's unique ID.
SF-992247 ACM-76647	A rejected change request approval step did not display when the workflow had completed.
SF-1046799 ACM-79688	Workflow decision nodes always evaluated manually entered variables as false.
SF-906005 SF-1008529 SF-996290 SF-944962 ACM-71857	An SQL error occurred when saving changes to an existing workflow process if it contained a delay node that was created in an earlier version of the product.
SF-914725 ACM-72045	A workflow copied from another workflow did not carry over the email body of the "Send Email" node.
SF-1062447 ACM-81011	Changes to due dates, priorities, and status could use cached data instead of the updated data.
SF-1070592 ACM-81877	Email approval templates incorrectly encoded the Email Approval Reply text.
SF-1031265 ACM-81002	The Workflow configuration to select 'Use Process configured on' was not available in the drop-down options after they paged.
SF-1096258 ACM-83234	The event type "Reject Changes handled by this workflow" was not available for Cancel Change Request nodes.
SF-1018709 ACM-79677	The email fulfillment handler did not contain an option to edit the email body or add workflow variables.
SF-1101627 ACM-83545	A Delete Account change request could be marked as complete but still show a status of "Pending Action".
SF-1098925 ACM-83236	Imported legacy workflows created before version 7.0.1 had a legacy value not handled by the new architect editor.

Collector

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

Issue	Description
ACM-70748	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.
SF-792018 SF-843886 ACM-63785	The activity owner did not save when creating a local entitlement collector. An edit was required to add the activity owner.
SF-964094 ACM-76458	After installing RSA Identity Governance and Lifecycle, the identity collector would not connect to Novell IDM.
SF-991315 ACM-76565	For a change request that failed due to an invalid CR_ID, the review submission did not roll back updates to the database as expected.
SF-1003979 ACM-77722	The application metadata collector could not use the "category" attribute of an application for collections.
SF-999750 ACM-76886	Deactivating an existing data access collector from the General tab discarded settings for user and group resolution rules.
SF-00909993 SF-00907746 SF-00906213 SF-00915126 SF-00917341 SF-00929895 ACM-71772	ADCs are failing with the following error: "Unprocessed Continuation Reference".
SF-795126 ACM-62974	Application metadata collections of wrong date formats for date attributes caused collection failures.
SF-1048233 ACM-80958	When using the Test button on a SQL query for a database collector, the screen incorrectly displayed a SQLException for a valid SQL statement.
SF-954031 ACM-78053	The transformer did not correctly create a CSV file for the CyberArk application.
SF-1039961 ACM-79634	The Salesforce collector did not collect LastLoginDate as expected due to an invalid date format error.
SF-1058274 ACM-80940	The WorkDay collector was failing with the following error: "Unmarshalling Error: unexpected element."

Connector

Issue	Description
SF-882233 ACM-71264	When a chain of certificates was involved in the handshake, the SOAP connector failed over 2-way SSL.
SF-877139 ACM-70139	Attribute values edited to be blank did not carry over to the connector in attribute synchronization.
SF-966500 ACM-75158	Stored procedures called using a DB2 connector returned a null pointer exception.
SF-947029 ACM-74335	Unable to create a connector with a generic database using the DB2 connector template.
SF-973647 ACM-75745	AFX Connectors did not deploy when the connector dependency file ID exceeded 999.
SF-862539 ACM-70218	Disabled users were enabled after a password reset.
SF-973760 ACM-75597	The Archer connector did not deploy when the password to access had $ in the string.
SF-965812 ACM-75343	AFX requests for account creation fulfillment did not succeed due to "no signature of method" errors on the SOAP webservice connector caused by an encrypted password.
SF-1030498 ACM-79568	The SAP AFX Connector did not decrypt passwords when creating an account, preventing login with the password assigned.
SF-1045422 ACM-79915	The Lieberman EDC did not save the value for the Domain Name parameter.
SF-927034 ACM-73176	Users with multiple accounts in the same Active Directory database could not sync their passwords.
SF-807227 SF-1095978 ACM-64072	The Oracle AFX connector failed when a password contained the $ special character.

Custom Attributes

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

Dashboard

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

Data Collection Processing and Management

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

Issue	Description
SF-957979 ACM-73932	
SF-955199 ACM-74460	Indirect Relationship processing did not reliably succeed because of Oracle error ORA-30926.
SF-954489 ACM-74783	A custom user-type attribute of a business source could get resolved to a terminated user if the custom attribute value did not distinguish the active or terminated user status.
SF-729636 ACM-57408	The MAEDC did not reject references to local applications.
SF-976294 ACM-75655	Indirect relationship processing of account changes for an ADC had performance issues and did not succeed when processing new account relationships.
SF-819318 ACM-65066	The collector did not allow edits because one of the collection data run tasks showed "in progress," but no collection was actually happening.
SF-910243 ACM-71796	When a moved column value was too large for the new field, indirect relationship Processing for the Data Access Collector did not succeed due to error ORA-12899.
SF-993679 ACM-76572	A data type difference between two tables caused IDC Collector to not successfully collect due to ORA-01722: invalid number.
SF-985280 ACM-75977	A Change Verification job ran a long time for the Attribute Synchronization watches.
SF-964401 ACM-74754	The "Collect Identity" dialog box for selecting only non-mandatory collectors incorrectly implied that unification would run after collection.
SF-945246 ACM-74003	Collector configuration could not be modified, even when collection was not actively running.
SF-996452 SF-1008697 ACM-76856	Identity unification did not succeed because duplicate users caused unstable rows in the source tables.
SF-999529 ACM-77260	The group owner had to be processed again in later collections after a group collection did not resolve group owner values to a user.
SF-939467 ACM-73665	A collector may not finish processing due to error "java.lang.ArithmeticException: / by zero" when one of its internal processing files was between 8192 and 8195 bytes in size.
SF-991460 SF-998540 SF-752747 SF-981434 SF-902733 ACM-76508 ACM-60176 ACM-75770	Collected IDC attributes were not being properly applied to the unified user.

Issue	Description
ACM-77967	
SF-853028 ACM-68135	The entitlement collector, when using a MySQL database as a source, did not correctly collect the approle memberships and entitlement relationships.
SF-1025190 ACM-78293	The application metadata collector did not successfully run on a database with a large history of data runs.
SF-985551 ACM-76498	During IDC processing, new users were sometimes not properly processed into the table T_RAW_USER, and this caused missing unified user attributes.
SF-831492 ACM-66204	Collected user accounts mapped to unique identity attributes, such as email address, were not unmapped and orphaned when the value of the identity attributes changed.
SF-758832 ACM-62291	When the truncate data option is selected, strings with multi-byte data are not properly parsed.
ACM-78555	Benign errors stating "unable to find an attribute length" displayed in the logs when running collections.
SF-906377 ACM-77158	In some cases, users moved from lower priority IDC to higher priority IDC (and vice versa) created duplicate identities in the data.
SF-944339 ACM-73752	When importing a user account mapping for an orphan account, the new mapping was not reflected in the Total Orphan count in the application’s General tab.
SF-1044348 ACM-80237	Unification did not complete due to duplicate entries that caused unstable rows in the source tables.
SF-1027126 ACM-78580	The ADC occasionally performed poorly in runtime when validating data on step 2 of pre-processing.
SF-1073461 ACM-81946	User access table could not show entitlements of manually mapped accounts.
SF-628040 SF-680992 SF-654543 SF-690382 ACM-54093	Collection of AD date-time attribute values did not properly convert to the Aveksa server time zone.
SF-1018130 SF-1034638 ACM-79114 ACM-78727	User type attributes did not correctly display the User name, but showed the ID instead.
SF-1083500 ACM-82456	Excessive memory usage during RDC processing caused the Oracle error "ORA-04030: out of process memory”.
SF-1072789 ACM-81847	After an upgrade, an Oracle error for an oversized column occurred when running the ADC and calculating relationship changes.
SF-746902 ACM-58736	The long business description of an application did not show on the editing screen after it was collected.

Issue	Description
SF-1055180 ACM-80332	Unification performance issues occurred in an IDC hierarchy with multiple joins.
SF-1077479 SF-906377 ACM-83014 ACM-77158	Unification duplicated users with new records and terminated the original users when users moved from one IDC to another.
SF-1058100 ACM-80563	When a user was moved from one IDC to another, unification terminated the original user and created a duplicate user.

Data Governance

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

Database Management/Performance

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

Issue	Description
SF-956468 SF-1004793 SF-1011605 SF-1017008 SF-1030278 ACM-58925	
SF-795053 SF-883282 ACM-55401	The Aveksa Statistics Report did not report the correct sizes in the internal table summary.
SF-977818 ACM-75607	The V_DC_LATEST_FAILED_RUN view did not include collections that failed on circuit-breaker.
SF-1082570 SF-1091399 ACM-82474 ACM-82979	Exports through either the command line or the user interface failed if the process was previously interrupted and then started again.

Descriptions

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

Email

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

Issue	Description
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.
SF-988027 SF-997491 SF-973366 SF-969211 ACM-76487 ACM-76609 ACM-76601 ACM-75170	International characters in HTML data prevented saves of email templates and email nodes.
SF-977178 ACM-75978	Excessive PasswordResetEvent and PasswordExpirationEvent ERRORs filled the aveksaServer.log file and delayed startup and shutdown.
SF-1004206 ACM-77308	Password resets issued by the administrator sometimes incorrectly displayed a 3-character password for the user accounts due to special characters in the view page.
SF-1010051 ACM-77547	When the email template AdminErrorNotificationMail is modified, that template could not populate the variable fields in the body when sending the admin Error email.
SF-932643 ACM-73930	Email events generating emails in a non-English could not change the language of the hyperlink text from English.
SF-1014915 SF-1014903 ACM-77735 ACM-77736	An encoded approval response was sent to a change request email approval.

Installer

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

Issue	Description
ACM-76587	
SF-872354 SF-877589 SF-888160 ACM-69405	During a new installation, if the Oracle UID, oinstall GID, or both are not the default value of 500, the install script performs chown -R /tmp/Aveksa/staging to oracle:oinstall, regardless of the current ownership.
SF-1045387 ACM-79591	An XML parsing error occurred in UI settings data for a given user when applying a patch.
SF-1052918 SF-1063628 ACM-81060	The Oracle error ORA-01439 stopped initialization due to custom attributes with incorrect data types.
SF-1078101 SF-1053551 ACM-81325	The patch build number did not update after applying a patch, which caused patch processing to reoccur at startup.
SF-970037 ACM-76001	Duplicate files in aveksa.ear caused errors when deployed.
SF-942673 ACM-73935	The installation or upgrade process would get stuck when one or more required install packages were missing.

Localization

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

Metadata Import/Export

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

Migration

Issue	Description
SF-950767 ACM-74441	The custom user attribute SUPERVISOR_NAME conflicted with an existing, identical attribute during a schema migration.
SF-976839 ACM-75848	During migration, the file ACM-60520.sql was running for several hours.
SF-974378 ACM-76009	An upgrade from 7.0.1 p2 to 7.0.1 p3 caused error "ORA-30926: unable to get a stable set of rows in the source tables" while executing the script database/migration/migrateReviewData.sql.

Issue	Description
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.
SF-904759 ACM-71406	The migration screen did not clarify that the build versions shown refer to the database schema versions.
SF-897425 SF-995347 ACM-71062	A null pointer exception error could occur while viewing the migration webpage after clicking the "Follow Output" link.
SF-1098141 ACM-83172	Benign Oracle error ORA-06502 appeared when upgrading from an earlier release.

Password Management

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

Reports

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

Issue	Description
SF-847594 SF-916311 ACM-63502	
SF-978571 SF-992545 ACM-75807	A generated report did not use a new filter after it was applied.
SF-997123 SF-1041210 SF-1060770 SF-1060627 ACM-76633	The Aveksa Statistics Report generation stalled indefinitely after an XML parsing error.
SF-893547 ACM-71068	Text in the header row of a report was cropped and unreadable when a large number of columns were present.
SF-946294 ACM-73894	Sorting the reports table by the "Last Modified" column resulted in no reports being listed.
SF-973770 SF-1024500 ACM-75652	A custom scheduled report displayed results without applying requested modifications to the SQL query.
SF-1050335 ACM-80389	A user summary table took longer than expected to download from the UI.
SF-962852 ACM-74715	When trying to filter by group name in the Group Memberships report, the popup picker showed the list of report definitions instead of group names.
SF-868021 ACM-70441	The Global Roles Summary by Owner report erroneously included deleted roles.

Request Forms

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

Issue	Description
SF-887157 ACM-70735	Newly created Provisioning forms did not have user variables available in the list of form fields.
SF-843527 ACM-67287	Fields could not be added to a request form using a web service with basic authentication.
SF-1010503 ACM-79564	A change request would not reflect a change in previously checked entitlements when using the back button to change the entitlements table filter provided from another component.
SF-1044516 SF-1047015 ACM-79555	When the user interface was displayed in Portuguese, the date selector did not work.
SF-1079363 ACM-82831	The Password Reset form only created change items for passwords and did not process field components that created other kinds of change items.

Role Management

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

Issue	Description
ACM-57064	
SF-792647 SF-836164 ACM-65704	Role status remains in Applied or Applied New State, even after change request is complete.
SF-856943 ACM-68009	The exports of a large number of roles timed out before successfully completing the task.
SF-1007760 ACM-77310	A user without access to a role's assigned roleset could remove the unseen roleset when editing the role.
SF-987405 ACM-76935	The UI incorrectly displayed the raw role name instead of the role name on the Apply Changes and Commit Changes To Roles screens.
SF-1046008 ACM-80259	Local Entitlements could be deleted when associated with a role in the "New" state.
SF-1011117 SF-999469 SF-1001009 SF-1030252 ACM-77717	Entitlements could not be added to business roles due to an internal Oracle error.
SF-1067573 ACM-81344	Curly braces in the Column IDs table caused errors when sorting users by "Role Out of Constraint".

Rules

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

Issue	Description
SF-1060767 SF-1024622 ACM-80583 ACM-78296	The termination rule did not generate the expected change request to disable manually mapped accounts.
SF-1045601 SF-1060217 ACM-79609 ACM-80718	The termination rule incorrectly generated change requests to disable accounts that were not assigned to a user.
SF-1017682 ACM-80224	The Attribute Change rule failed with an exception when generating a change request to add a local entitlement.
SF-1042701 ACM-79712	The Attribute Change rule did not generate a review when there is an existing review generated by the rule in an active or hold state.

Security

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

User Interface

Issue	Description
SF-636368 ACM-52265	Color coding set as default by all users for rows defined by Control Type: Entitlement Table was lost if the user unchecked the Entitlement Type field in the table options.
SF-855386 SF-887226 ACM-67958	When using Internet Explorer 11 with Compatibility View or Enterprise Mode, the violation Revoke and Maintain buttons were disabled.
SF-1027542 SF-1022950 SF-1017658	Could not log in to version 6.9.1 using Compatibility View in Internet Explorer 11.

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

Web Services

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