RSA Governance and Lifecycle

V7.0.0 Patch 3 Release Notes

Contact Information

Go to the RSA corporate website for regional Customer Support telephone and fax numbers: www.emc.com/domains/rsa/index.htm.

For technical support, contact RSA at support@rsa.com.

Trademarks

RSA, the RSA Logo, and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC 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 EMC, 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 EMC.

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 Governance and Lifecycle product and selecting the About menu.

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 EMC software described in this publication requires an applicable software license. EMC 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." EMC CORPORATION 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.

Revision Date: May 2016

Contents

Install a Patch

This section explains how to apply a patch to RSA Governance and Lifecycle appliance and soft-appliance installations and how to upgrade Access Fulfillment Express (AFX) connectors. Patches are cumulative.

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

Considerations

- Database: This advisory applies only to patch upgrades for installations that use a remote customer-supplied database. The patch process may run SQL against various tables in the database. Consequently, no database procedures should be running against the remote, customer-supplied database schema during the patch installation. Make sure the database is idle before applying the patch.

  Note: For an appliance with a local, RSA-supplied database, the patch script will stop and start the local database to insure that this requirement is met.

- Clustered Environment: If you are running in a clustered environment, only one node must be used during the patch update process. Stop all other nodes in the cluster to avoid multiple nodes attempting a database migration. Validate the patch has been applied and the one node is working as expected before patching other nodes in the cluster or enabling farming to push ear changes to other nodes.
- WebLogic: The patch requires RSA Governance and Lifecycle to be re-deployed. See the *Installation Guide* for instructions.
- WebSphere: The patch requires RSA Governance and Lifecycle to be redeployed. See the *Installation Guide* for instructions.
- Wildfly: The patch contains a deployment script, patch.sh, to install the patch..
- AFX Connectors: If you are running AFX, this patch release includes updated connector packages. You must download and import the packages. See the instructions below.

Install the RSA Governance and Lifecycle Patch

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

Important: Installing a patch overwrites all custom configuration settings for AFX servers (JVM settings for example). You must manually restore the settings after the import.

Procedure

1. If you have AFX installed, using the AFX user account, shut down all of the AFX instances before installing the patch upgrade:

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

2. Download the following files available from RSA SecurCare Online at https://knowledge.rsasecurity.com:

   - RSA_Via_L-G_Release_Notes_<VersionNumber>.pdf
   - Aveksa_<VersionNumber>_P<PatchNumber>.tar.gz

3. Uncompress and untar the file. Run the following commands:

   a. `cd /home/oracle`

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

4. Log in as root and run the patch.sh installation script in the directory created in Step 3. Run the following commands:

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

   b. `sh patch.sh`

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

   ```
   acm restart
   ```

Download and Import AFX Connector Packages

Use this procedure to download and import the AFX connector package.

Procedure

1. Download the Connector package files available from RSA SecurCare Online at https://knowledge.rsasecurity.com 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

2. Log on to RSA Governance and Lifecycle.

3. Click AFX > Import.

4. Import the packages.

5. Run the following command:

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

Release 7.0.0 Patch 3

Information about the 7.0.0 Patch 3 release is included in the following sections:

- What's New in Release 7.0.0 Patch 3
- Fixed Issues in Release 7.0.0 Patch 3

What's New in Release 7.0.0 Patch 3

Feature	What’s New
Access Requests	A web services command "Terminate User". This command is an improvement to the createChangeRequest command. This command allows any user who has access to terminate a user, to do so through a web services call.
Access Requests	Added UserID as a default column and user attributes in the available columns in table options.
AFX	The primary communication poll from AFX has been optimized for better performance.
Attributes	Added new Custom Attribute Type for URL support. This allows an admin to create a custom attribute to include a link that opens a specified URL. For example, if you have created an external page that interfaces with RSA Governance and Lifecycle, you can use this attribute to launch a pop-up with additional information.
Collectors and Connectors	The ServiceNow collectors and connectors are now compatible with Eureka and FUJI versions of ServiceNow.
Collectors	The Lotus Notes entitlement data collector has been enhanced to increase collection efficiency. The Lotus Notes entitlement collector supports collection of a replica ID that is mapped to a custom attribute. This allows you to collect all the versions of applications from different Lotus Note databases
Connectors	Added connector support for Salesforce API v36.0. The Generic REST connector supports HTTPS connection to a Zendesk endpoint. The generic SOAP connector is available for AFX.
Database Index	Created an index for the WP_WORK_ITEM table to help organize the Dashboard queries. The columns are displayed in the index in the following order:

Feature	What's New
	• name • work_state_id • app_ref
Workflows	RSA Governance and Lifecycle's Workpoint implementation has been upgraded to version 3.5.2. The workflow editor now has filtering, split count circuit breaker, iteration limit features for multiple monitors, and more detailed history logs.
Workflows	Only workflow work item history is accumulated. This prevents unnecessary accumulation of workflow data in the database
Workflows	The option to reset the job was removed from the Job menu in workflows.

Fixed Issues in Release 7.0.0 Patch 3

Issue	Description
SF-650965 ACM-53908	When configuring the REST Web Services Connector, the Command Code Path input field cuts off all of the content after the "&" character.
SF-783309, 766351 ACM-61786	The field "Security Token" appeared mandatory in the new SalesForce Data Collector configurations.
SF-773609 ACM-60921	RSA Governance and Lifecycle is not displaying dashboards according to the display sequence.
SF-777489 ACM-61686	After upgrading from 6.8.1 P20 to P22, the "The request could not be handled" error appears in the General tab when the attempting to edit or create new reports.
SF-711897 ACM-55731	AFX connectors do not install when imported from a development box to a test box in a WebSphere environment.
SF-779263 ACM-61776	When trying to run the Register User request form configured with the Naming Policy having a single attribute transform, a "Missing two input values" error appears.
SF-783596 ACM-61770	Leaking CLOBs and XMLType exceeded maximum temporary space over a period of time.

Issue	Description
SF-620305 ACM-52017	Terminating a user using the Default Terminate Button, Default Terminate Form, or default workflow duplicates change requests.
SF-771497 ACM-61396	User access review items are unassigned after uploading the coverage file that specified reviewers.
SF-696093 ACM-54926	Group entitlements are unassigned in the user access review.
SF-773391 ACM-62617	Role ownership resolved to previously deleted user.
SF-762813 ACM-60776	The field in the Entitlement Data Collector table was not big enough to support concatenating Resource Name and Action fields.
SF-746921 ACM-58879	If the change request is stuck with no created workflow, closing the change request keeps the roles in the applied state rather than reverting them.
SF-760448 ACM-60355	Scheduled backups are not executing automatically.
SF-752280 ACM-60146	When writing users from RSA Governance and Lifecycle through join request into an identity source, users with an apostrophe in their name get a double apostrophe.
SF-751641 ACM-59393	The Operator, under the Update managed attribute value check box, does not set the value to the current date when Set to detection date is selected.
SF-784527 ACM-62533	Selecting Account Creation Date multiple times in the Table Options, duplicates the columns in the Change Preview tab.
SF-791879 ACM-62654	An error message appears when the Decision node connects the Fulfillment Phase Node and Form Fulfillment Node. The fix now allows a Decision node between the Fulfillment Phase Node and Form Fulfillment Node.
SF-777749 ACM-61791	In the Exceptional User Access Workflow, the Maintain All, Revoke All, and Clear All buttons are not functional for the Secondary Rule Remediation node.
SF-632425 ACM-52120	An SQL injection threat is observed when importing a workflow.
SF-803677	A workflow stays in the Created state until it is manually evaluated.

Issue	Description
ACM-63495	
SF-755785 ACM-61422	In the Applications > Account tab, The table column does not display Custom Attribute Integer 4 (CAI4) after the data was collected.
SF-741584; SF-795450 ACM-62634	The Dashboard shows the default review tabular report instead of a tabular report specific to the review that is being viewed
SF-803077 ACM-63479	The User Accounts table is not displayed in forms that have a condition associated with a table, even if the condition is valid.
SF-803077 ACM-63981	The configuration of hidden fields in a request form is causing an error condition when a requestor attempts to create the request.
SF-738151 ACM-56484	The Salesforce.com AFX connector is not working with Salesforce API 34.0 to create an account for Salesforce.
SF-770400; SF-756694 ACM-60732	MAL: The connection to remote agents timeout, interrupting the collection process.
SF-796872 ACM-62981	When creating a request form for a new group access for UNIX platform, the Entitlement Name field appears as not required.
SF-793954 ACM-62731	A workflow statement fails with an "Invalid column index" error.
SF-793794 ACM-62780	Unification fails at step 5/10 with this error: "ORA-30926: unable to get a stable set of rows."
SF-798500 ACM-63319	Installation of 7.0.0 Patch 01 over 7.0 failed.
SF-792812 ACM-62643	The entitlement data collector does not work with a custom database driver after the upgrade.
SF-740094, SF-740342 ACM-61117	Based on the number of remediators, duplicate work items are displayed under the Violation Remediation tab.
SF-791875	When a selected user does not populate any accounts into the table, the "User

Issue	Description
ACM-62506	Account Table" field, in the request forms, returns a "required" warning, even though it is not configured as a required field.
SF-785022 ACM-62505	A user review shows the direct membership of nested roles.
SF-787727 ACM-62247	A report was not imported properly, resulting in the bind variables default values not appearing on the query page of the report.
SF-660715 ACM-53471	A Lotus Notes entitlement data collector run is not optimal and requires extensive permissions.
SF-775070 ACM-60987	Unable to assign remediators to unassigned rule violations.
SF-697411 ACM-55178	The account collector search scope only returns the first group and member of the group.

SF-766469;
SF-782885;
SF-764569;
SF-805030
ACM-61621
	Aveksa EAR file is not generated in the /home/oracle/archive path.

SF-788716 ACM-62503	During migration to 6.9.1 P7 and above, the migration script produced duplicate data in the UNDO tablespace, causing the patch installation to fail.
SF-800215 ACM-63298	Identity collector indirect relationship processing taking seven hours and deleting user relationships.
SF-782388 ACM-61635	An "ORA-01000: maximum open cursors exceeded" error occurred when a report was generated.
SF-778033 ACM-61355	Patch installation failed in a 7.0 Wildfly software appliance installation scenario.
SF-808504 ACM-64046	A "Driver Class cannot be empty" warning appears when configuring an account collector with a Custom database type.
SF-801042 ACM-63358	Account collection is taking an inordinate amount of time to complete.

Issue	Description
SF-785277; SF-808843 ACM-62821	SQL command in a Workflow node not properly ended.
SF-791651 ACM-63736	Valid query in workflow node fails.
SF-776459 ACM-62468	In custom tasks, "Can Run Manually" and "Administrator can run manually" filter conditions were not working. Now, "Can Run Manually" lets the user listed in the filter run the task with the 'Run' button enabled. "Administrator can run manually" now considers the user as an administrator if he or she has an App Role as a Access Request Admin.
SF-21843 ACM-48378	Workflow SQL parser is unaware of quote delimiters when using form variables.
SF-783226, 803077 ACM-62595 ACM-65223	Several user interface elements are "grayed out" when using Internet Explorer after an upgrade to 6.9.1 p10. The browser used a locally cached version of JavaScript files after the upgrade.
ACM-65490	An error occurs when a workflow reference variable is used in an SQL node in a fulfillment workflow.

Release 7.0.0 Patch 2

Information about the 7.0.0 Patch 2 release is included in the following sections:

- What's New in Release 7.0.0 Patch 2
- Fixed Issues in Release 7.0.0 Patch 2

What's New in Release 7.0.0 Patch 2

Feature	What's New
AFX	AFX can use the TLSv1.2 protocol for all outbound HTTPs requests to an L&G server that has TLSv1.2 enabled for inbound connections to port 8444.
Collectors/Connectors	Enabled TLS 1.2 support in V7.x and above for the Salesforce collector /connector because Salesforce is disabling TLS 1.0 support.
Collectors/Connectors	The CyberArk collector/connector components are included in this patch release.
Custom Attributes	The "Application" object in Admin > Attributes > Custom List includes a third option, "Name." It lets you provide an alternative business-understandable name in addition to the Raw name.
Rules	Under Rules > Configuration > you can configure standardized justifications (written statements) that rule violation remediators can apply when they confirm that they want to maintain exceptional access for users with violating access. The benefit of implementing justifications is that they enable you to provide well-written, clear reasons for maintaining exceptional access using a vocabulary that other stakeholders in your organization can understand rather than relying on whatever free-flowing text a remediator may provide. For example, you may want to create justifications that express reasons such as the following.: • This violating access is maintained because the violating access is benign and will expire in three days. • This violation access is maintained because the violating access is benign and will be revoked in the upcoming access certification review. How you manage and work with justifications: • You can create as many justifications as you require, and then group them into any number of justification sets you create.

Feature	What's New
	- You can apply a justification set to any number of user access and segregation of duties rules, and you can apply any number of justification sets to these rules. You cannot, however, apply more than one justification set to a rule's violation remediation action configuration. - Any changes you make to a justification set (adding or removing justifications, editing justifications in the set) are in effect immediately for all rules to which it applies. How rule violation remediators apply justifications when they grant exceptional access: - When a remediator is prompted to confirm the exceptional access, he or she must select a justification from the Justification field. - The remediator can also choose to enter additional comments for his or her action in the Business Justification text-entry field. - If justifications are not specified for the rule that detected the violating access, the remediator is required to enter comments in the Business Justification field.

Fixed Issues in Release 7.0.0 Patch 2

Issue	Description
SF-700719 ACM-55535	Users lose the "Other Business/TechnicalOwner" or "Other Violation Manager" entitlements to business sources when a business source that had these entitlements granted to users is deleted.
SF-769891 ACM-60586	The "Data is case sensitive" setting for an account collector is ignored, resulting in 40,000 orphaned accounts.
SF-763198 ACM-60872	Manual account mappings are not cleared after collected data indicates they should be cleared.
ACM-61037	Modifyhostname.sh has relative paths.
SF-763568 ACM-60657,	ServiceNow Collector runs successfully on first run, then continues to fail.

Issue	Description
ACM-60633	
SF-749898 ACM-58642	AFX download server delivers a zero size file when there us not enough space user /tmp. This error was indicated in the log file, and is now also shown in the user interface.
SF-772393 ACM-61086	An account review is completed but the Completed Status bar indicates that it is not completed.
SF-777383 ACM-61303	Specially constructed URLs could allow information leakage vulnerabilities where a user could view information for which they do not have privileges. This issue was fixed.
SF-619882 ACM-51714	BindPassword of authentication source is now obscured properly.
SF-684046 ACM-54433	Values for a drop-down control in request forms cannot be deleted if the value contains quotes
SF-615728 ACM-52615	When the account is switched to Maintain state, the account sub-components become actionable and when the account is Revoke state, the account sub-components become locked.
SF-20142 ACM-46894	Groups that are direct or indirect entitlement to the role are not filtered out by the "not in Role with" option in a group definition review.
SF-777907 ACM-61295	When filtering business sources in the review definition, using an SQL statement with new lines in the query leads to an ORA error during review generation on Weblogic.
SF-775143 ACM-60989	When the big role changes are requested, it takes a long time to create the change request.
SF-758073 ACM-59428	The entitlement collector fails during the database processing stage.
SF-767428 ACM-60387	The A_AVR_ACCOUNT_ENTITLEMENTS view is deleted after running a collector a second time.
SF-764480 ACM-60052	Customer cannot use the word 'Replace' as part of the SQL query in the Entitlement collector.
SF-763404	A change request to commit changes to a role takes an inordinate amount of time to

Issue	Description
ACM-59907	complete.
SF-757246, 757712 ACM-59587	Users with null on unification join attribute are rejected. The following unification error is observed: "EC[102] Context[RunID=60245, IDC(ID=21)] Message[Identity Data Validation: One or more attributes user in Join Condition has duplicate values.]"
SF-771363 ACM-60734	Entitlements cannot be mapped to users if a multi-app entittlement collector is deleted.
SF-767681 ACM-60520	Unification and Aveksa ADC processing never completes after applying 7.0 P01. Both tasks are required to be canceled using the Kill Task option in the Run Details page under Admin > Monitoring.
SF-744512 ACM-57938	Review generation is very slow after the migration from version 6.8.1 P11 to 6.8.1 P21.
SF-771705 ACM-61364	When the first step does not get generated, the second step review generation fails with unique constraint error.
SF-765036 ACM-60137	After upgrading to v6.9.1.09, RSA Governance and Lifecycle startup fails due to SSO error. This issue has been fixed.
SF-694923 ACM-54944	Language in advanced search remains in English even when the language is changed in the Options link.
SF-775598 ACM-61116	A "Request could not be handled" error occurs when attempting to download a statistics report.
SF-775551 ACM-61215	Submission variable is not appearing on all Change Requests, when the Change Request uses a custom form with grouping by user and multiple users are submitted. This issue has been fixed so the variable now appears on the Change Request for each user.
ACM-56202	With Novell IDM Entitlement Data Collector, entitlements were resolved against Users, but now entitlements are being resolved against Accounts.
SF-766469, 782885, 764569 ACM-61621	Aveksa ear file is not generated in /home/oracle/archive.
SF-754154,	Cannot collect from a cloud-based Workday application without the ability to

Issue	Description
771853 ACM-59329	define web proxy.
SF-713802 ACM-55974	A Long Description hyperlink does not open in a new window/tab, rather the current window is replaced by the hyperlink URL.
ACM-46752	The "Data is case sensitive" setting for account data collectors does not work. Account data collection is case sensitive in all situations. For example, if the collector collects an account named "finance" and the name of the account is later changed in the data source to "Finance", the original finance account is deleted and a new Finance account is created.
SF-749705, 757128 ACM-58548	The server takes an long time to start and migrate the .jrxml files.

Release 7.0.0 Patch 1

Information about the 7.0.0 Patch 1 release is included in the following sections:

- What's New in Release 7.0.0 Patch 1
- Fixed Issues in Release 7.0.0 Patch 1

What's New in Release 7.0.0 Patch 1

Feature	What’s New
AFX Connectors	The Salesforce connector supports dynamic variables for its Create Account command. A connector for IBM Security Identity Manager (ISIM) is available.
Request Forms	The User Picker control type includes enhancements to the following ID value types: • Id — Returns a user's internal value from the product database. • Unique Id — Returns a user's value collected from the data source. • User Id — Returns a user's user name value from the product database.
Rules: Escalation Workflow	The ability to configure automatic revocation of violations after a particular escalation deadline is reached. Components: A "Rule Revoke Violations Escalation" workflow is available under Rules > Workflows > Escalation tab. It includes a single node, the "Rule Revoke Violations" node. The workflow can only be used for remediation escalation within a rule remediation workflow. How it works: You specify a due date escalation value for the Default Rule Remediation Action workflow. You want the workflow to invoke the Rule Revoke Violations Escalation workflow that detects violations that have not been remediated by the due date. If it detects non-remediated violations, the Default Rule Remediation Action workflow generates change requests to revoke the violating access. Set up: 1. Open Properties for the Default Rule Remediation Action workflow (or any custom version of it you have created). 2. Under the Due Date tab, select the Rule Revoke Violations Escalation workflow as the Workflow value for the Due Date value you specify.

Feature	What's New
Rules: Testing	The Provisioning - Termination and the Provisioning - Joiner/Mover rule definitions include a Test button. It allows you to test the rules just you can for User Access and SoD rules.
Rules	Tables that list users with violating access enable you to sort, group by, and search on custom attributes for those users.
User Access Review	The "Allow Group to be expanded to display access" option allows a reviewer to display the access provided by a group to a user. Reviewers can take action on the group, not selectively on the entitlements in the group. This enables the reviewer to determine whether to maintain or revoke the access provided by the group
Request Forms	RSA-provided forms are tagged as belonging to the "Default" category.
Enhancement of Authentication Type "SSO User Header"	If you want to validate an "SSO token," then as part of creating the authentication source of Authentication Type "SSO User Header," you must: 1. Provide the header name that contains the "SSO token." 2. Create and deploy a Java class that implements the 'com.aveksa.external.SSOTokenValidator' interface. This enhancement also facilitates web service calls that need to pass a valid "SSO token" instead of a password. For more information, see the "SSO User Header/Principal Configuration" SSO User Header/Principal Configuration topic below.

SSO User Header/Principal Configuration

This section is an addendum to the topic "Creating a New Authentication Source" in the Help.

- UserNameHeader — Enter the name of the header used to obtain the authenticated user name. When a request is sent to RSA Governance and Lifecycle, the SSO authenticator determines whether this is a proxied request by verifying the existence of this header name. Using this header name, the SSO authenticator authenticates the user by checking if the value in this header is present in the RSA Governance and Lifecycle users table. Any attribute of a unified user can be configured to perform this comparison. The user is then authenticated and an RSA Governance and Lifecycle session is created for the user.

- IpAddresses (optional) — Enter a comma-separated list of individual IP addresses from which the SSO authenticator will process requests. Typically, you can leave this field blank to indicate that all IP addresses in your network are allowed. This setting is useful if you want to lock down the SSO authenticator to honor requests from a single proxy.
- UnifiedUserColumn — Enter the name of the column in the Aveksa unified user table in which the authenticated user is compared. For example, USER_ID.
- RedirectURL (optional) — Enter the HTTP(s) URL in which the user is re-directed due to a failed login attempt. It must contain the macro %redirecturl% in the string (such as, https://myserver.mydomain.com?%redirecturi%). For example, if the header is found; however, there is no match in the RSA Governance and Lifecycle unified users table (or more than one match), then one of the following occurs:
    - If the SSO authenticator is configured with this redirect URL option, the user is redirected to the specified URL.
    - If the SSO authenticator is not configured with this optional redirect URL option, the RSA Governance and Lifecycle login screen is displayed to the user.
- LogoffURL (optional) — Enter the URL for which a user is redirected to when logging off from RSA Governance and Lifecycle. For example, a user logs off by clicking the Logout button. If the SSO authenticator is configured with this Logoff URL option, the user is redirected to the specified URL so that the external session can also be terminated.
- If the SSO authenticator is not configured with this Logoff URL option, the user is logged out of RSA Governance and Lifecycle; however, the user session remains active on the external system. The external session might be used for a subsequent login unless the web browser is shutdown. RSA recommends that you configure this Logoff URL to point to a resource that destroys the external session so that during a logoff (apart from the RSA Governance and Lifecycle session being destroyed) the external system's session is also destroyed.
- IgnoreCase — Indicates whether the text case is ignored (Yes) when comparing the user header values to unified user columns.
- AuthenticatorClass — Enter the name of the class that is used for authentication. You should not modify this setting.
- TokenHeader (Optional) — The field applies to the SSO User Header type only. Enter the name of the header used to obtain the ssotoken name (this is the ssotoken that is available in the HTTP request, created by the original Authentication Provider, for example, RSA Via Access Manager.

If this field is present in addition to the validation of UserNameHeader as mentioned above, the SSO authenticator authenticates the user by verifying the SSO Token. You must write a custom SSO validation class which implements the SSOTokenValidator class to validate the token. Upon validation, the user is then authenticated and an RSA Governance and Lifecycle session is created for the user.

- Validator Class (Optional) — The field applies to the SSO User Header type only. Enter the name of the class that you created implements the interface validateSSOToken and passes in the third party supplied SSO Token. When a request is sent to RSA Governance and Lifecycle, this SSO authenticator determines whether this is a valid proxied request by verifying the existence of this class and invoking the validation method. For more information, see Create a Custom SSO Authenticator Class.

Fixed Issues in Release 7.0.0 Patch 1

Issue	Description
SF-735273 ACM-57068	Change requests in the system indicate they were generated by users who did not generate the requests.
SF-733148 ACM-57348	AFX fails to fulfill approved request items. The following error is observed: "ERROR (Worker_actionq#ActionQ1#WPDS_2) [com.aveksa.server.workflow.scripts.nodes.FormApprovalsNode] Error generating the approval and fulfillment nodes org.hibernate.exception.SQLGrammarException: could not execute query at org.hibernate.exception.SQLStateConverter.convert(SQLStateConverter.java:92)"
SF-20540 ACM-49006	A "Request could not be handled" error occurred when an attempt to invoke a role link from email in the Admin > Email > Log window.
SF-725668 ACM-56504	Multiple database deadlock conditions observed.
SF-646251 ACM-52579	The Review Definition: View All entitlement enables users to modify escalation settings.
SF-718060 ACM-	The URL link in rule violation remediation email does not display the violations.

Issue	Description
56342	
SF-706614 ACM-56277	Parallel SQL nodes in a workflow produce inconsistent results.
SF-663107, 642394, 654876, 660592, 677237, 677764 ACM-54809	Some role entitlements are incorrectly removed during subsequent collections.
SF-731259 ACM-56794	RSA Governance and Lifecycle 7.0.0 initial database setup fails with this error: "Unable to get database version.”
SF-727042 ACM-56813	A change request stalls in the approval node after processing over 1000 request items.
SF-657164 ACM-53336	Adding a node to workflow creates two instances of the node.
SF-596925 ACM-51030	The send email action is not executed for an attribute change rule.
SF-702306 ACM-55192	The Maintain and Revoke buttons in a review are unresponsive when French is designated as the default language for RSA Governance and Lifecycle.
SF-625568, 620646, 668423, 680413	False AFX failures occur when adding or removing user accounts from groups in Active Directory.

Issue	Description
ACM-52843, ACM-51871	
SF-627569 ACM-52088	Action buttons are disabled only for group owner reviewer when using the review results menu.
SF-725911 ACM-56545	Editing imported local entitlements changes entitlement names to entitlement raw names.
SF-643163 ACM-52537	Processing rules in one rule set processes all other active rules in other rule sets.
SF-690230 ACM-54602	The WebService cmd findEntitlements sortDirection parameter is not properly documented.
SF-711283 ACM-55815	Account collection taking an inordinate amount of time to complete after the account collector is configured to collect groups in addition to accounts.
SF-664551 ACM-54623	A user who rejoined an organization is not provisioned with the same entitlements he/she had prior to termination.
SF-710501 ACM-55667	A user who rejoined an organization is not provisioned with the role he/she had prior to termination.
SF-696638 ACM-54943	A "NullPointerException" error occurs when importing a rule definition that references a non-existent custom attribute.
ACM-55414	Remediation workflows are not created for all user access rule violations.
SF-684951	A change request to add access for a user is canceled at the approval phase if the user does not have a backup supervisor and the Supervisor Approval node in the

Issue	Description
ACM-55148	workflow has backup supervisor specified as one of the resources.
SF-705415 ACM-55485	Old change request identifiers are displayed for SoD rule names for violation remediation tasks under Admin > Workflows.
SF-678405, 700864 ACM-54309	A user who creates a change request is unable to cancel the request even though the request workflow is configured to allow cancellation.
SF-651276, 645804, 639819, 653846, 641001, 666533, 672358, 679297, 677862, 684959 ACM-52718	The Appliance tab on the Admin System page does not load.
SF-664872 ACM-53419	A change request does not close when the AFX workflow is configured with the "Create a job per group, grouping by user" setting.
SF-719788 ACM-56120	Infinite looping occurs after editing a role profile.
SF-690180 ACM-54591	A reviewer was unable to undo a sign-off on review items.
SF-689461 ACM-	There is an issue with the "Set_ChangeItem_Category" procedure.

Issue	Description
54662	
SF-700826 ACM-55870	An AFX fulfillment call after an approval did not occur.
SF-701486 ACM-55171	The Modify button is unavailable for users added to a review by a review refresh.
SF-697485 ACM-55072	Deleted user account mapping displays in the Reset My Password form.
SF-654610 ACM-53044	Role name changes from Role Set Name to Role Set Raw Name during the fulfillment process.
SF-698118, 681069 ACM-54989	An "Insufficient Privileges" error occurs when attempting to view a user's Request tab.
SF-689044 ACM-55312	Review email is not sent if one of the recipients has an invalid email address.
SF-692001 ACM-54672	When the name of an application role for a particular business source is changed, all equivalently named application roles for other business sources are changed as well.
SF-647629 ACM-52654	A problem occurs when attempting to create a business description for a set of application roles.
SF-698100 ACM-55120	Saved report results are missing after an upgrade from v5.1.4 to v6.9.1.
SF-691441	(WebLogic) Changes to the user interface display settings are not reflected across

Issue	Description
ACM-54738	nodes.
SF-697317 ACM-55069	Role definition reviews are generating change requests to revoke groups from users that are not members of the role.
SF-679345 ACM-54994	Asset Owner approval not working for entitlement of type account group. The approval is system-approved instead of being assigned to the asset owner.
SF-626239 ACM-51948	The Admin > System > Settings page shows inconsistent information when the database is remote and a local database has been imported.
ACM-54917	For the SoapWebService node, the proxy is not reset if cleared from the workflow node.
ACM-54431	When creating a new role and the fulfillment phase is set to group by user, the role remains in the Applied New state.
SF-680187 ACM-55131	A deleted role is included under a user's Access tab.
SF-694923 ACM-54944	Language in advanced search remains in English even when the language is changed in the Options link.
SF-705077 ACM-56002	Completed violating access remediation is indicated as pending.
SF-680826 ACM-54112	The MySQL connector does use the most current version of the jar file: mysql-connector-java-5.1.36-bin.jar
SF-19286 ACM-44975	Import of Business Descriptions reports the Modified By field as AveksaAdmin even if the import was performed by someone else.
SF-623248	Time out and performance issues occur with change request approvals.

Issue	Description
ACM-52021	
SF-692095 ACM-55130	Multi-app entitlement collections is taking over 18 hours to complete after installation of v6.8.1 p10.
SF-612345 ACM-51472	A request for an entitlement via an account for a user is rejected, yet the account appears under the user's Access tab.
SF-670181 ACM-53938	The AFX Salesforce connector did not support dynamic license variables.
SF-705986 ACM-55883	The Provisioning - Termination rule does not detect all terminated users.
SF-705698, 710766, 682951 ACM-55404	Cannot edit a SQL Execute node.
SF-702729 ACM-55196	An "ORA-01400: cannot insert NULL" error occurs when an SQL Execute node executes an insert on a not null type column in the database.
SF-21360 ACM-48408	There are duplicate breadcrumbs when drilling down in to requests, approval phase, and supervisor approval.
SF-679227 ACM-54820	An "HTTP/1.1 505 HTTP Version Not Supported" error occurs when attempting to select an application name that contains spaces from an access request form.
SF-685415 ACM-54692	Users are not displayed under the Who Has Access tab for an application.

Issue	Description
SF-545046 ACM-50059	A request submission question configured to display once is displayed multiple times.
SF-639987 ACM-52376	Password challenge questions are not localized for users' language choice.
SF-642293 ACM-53369	A Request form does not append the values in the non-visual fields when run to create an account.
SF-698511 ACM-55189	SSH Connector does not work when there are special characters in data from 6.9.1 P02.
ACM-53118	Some Aveksa application entitlements are not providing the privileges they are designed to provide.
ACM-55838	(WebSphere and WebLogic only) An error occurs when a unique ID value is used to search for a user in the Users table.
SF-696326 ACM-55082	Log in from an AD authentication source takes an inordinate amount of time.
SF-722232 ACM-56276	A requestor cannot proceed through a form if a required field that does not meet the display criteria is not displayed.
SF-538188 ACM-49730	The Requested On timestamp changes each time an approver clicks the Perform button for an approval.
SF-717733 ACM-56045	A null variable in email generated from a workflow displays as ' ' characters.
SF-714598 ACM-55859	When a technical role that is added to a global role is rejected, indirect entitlements of accepted technical roles are rejected.

Issue	Description
SF-681689 ACM-54567	Indirect items are fulfilled even if the role change direct item is rejected when the change request is created via role management.
SF-694001 ACM-55013	Change request with overlapping indirect entitlement items are rejected inconsistently when a role's direct items are partially rejected.
SF-731761 ACM-56814	A role's Analytics tab shows missing entitlements not actually missing after entitlement collection is run.
SF-728873 ACM-57591	Monitoring policies do not allow the user designated as the monitor to view account change requests for accounts.
SF-742983 ACM-57810	Escalation Workflow reassigned to the wrong Data Owner when a request contained approvals for more than one entitlement, and those entitlements had different Data Owners.
SF-730782 ACM-57594	In Requests > Request page, unable to edit a Change Request Workflow.
SF-732768 SF-737557 ACM-56957	In an approval workflow, group by selections does not work correctly. A single request appears twice in the group owner's approval list and sends two emails to the Group Owner.
SF-730334 ACM-56776	After a system restart, a change request is processed by the wrong workflow.
SF-728492 ACM-56703	In Requests > Configuration > Request Forms tab, when selecting and running a form, the User Picker - User filter using "avform" variable resets to "None."
SF-729843, 743321,	After submitting review items for sign-off, the Maintain and Revoke buttons remained enabled. These buttons are now "greyed-out" and not available when the review is submitted.

Issue	Description
ACM-56797	
SF-730311 ACM-56718	Requests are getting stuck in Open state, after adding an entitlement to a role. This issue was fixed so that such requests now move forward to the Approval stage.
SF-671161 ACM-54544	The "Entitlements Require Accounts" settings for applications are not exported in metadata.
SF-622727 ACM-52249	There is no rule escalation workflow that initiations revocation of violating access if that access is not remediated by a particular due date. For more information, see What's New in Release 7.0.0 Patch 1.
SF-741059 ACM-57735	The following workflow error occurs: "ORA-06512: at "AVUSER.ACCESS_REQUEST_PKG", line 314."
SF-659351, 710259, 714047 ACM-53308	Workflow error occurs when evaluating a SQL node that is not in the processing path.
SF-739244 ACM-58274	A multi-app account collector and a multi-app entitlement collector are granting access to other application accounts if the account name is the same.
SF-751429, 756354 ACM-58885	When using WebSphere JAAS and Via L&G Authentication, cannot authenticate to Active Directory on port 636.
SF-749097 ACM-58493	After installing 6.9.1.07, the installation seems to have completed, but after restarting services, the RSA Governance and Lifecycle user interface is not starting.
SF-759615	Role change request is created with wrong requestor.

Issue	Description
ACM-59522	

Known Issues and Limitations

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

Tracking ID	Description
ACM-62462	Applying Latest 7.0.0 P02 Build P02_7.0.0.106733, throws a java.sql.SQLException: "ORA-04068: existing state of packages has been discarded." **Workaround**: Restart the server and the application after you install the patch.
ACM-55216	A "Caught SQLException: ORA-00904: "STATE": invalid identifier" error occurs when a report is run.
ACM-55664	Entitlements of the type, global role, cannot be added to a role in a role set even though the Entitlement Rule setting for the role set allows that entitlement type to be added to the role.
ACM-56022	An entitlement collector from an AD source collects account-to-entitlement relationship is collected twice
ACM-52520	Only the Remove Change item is included in a request which was created to add and remove application roles for a user.
ACM-52471	When the Back button is selected in a request form, previously entered field values are not refreshed.
ACM-51564	The name of a reviewer selected in review definition disappears. It reappears in the review definition when the definition is subsequently saved and then re-opened for editing.
ACM-51562	Inconsistent bulk and single account review action results occur.
ACM-48298	When the "Allow Manual Activity to Complete before Collection" feature is enabled, the entitlement or application role is not added or removed.
ACM-48934	When a user selects "Cancel Change Request" with the "Reject Entire Request" event type selected, processed items are not rejected.
ACM-48962	The "Revoke," "Revoke All" and the "Maintain," "Maintain All" buttons are enabled in the View mode.
ACM-53322	A "request could not be handled" error occurs when attempting to modify a user access review definition's State option.
ACM-51465	A "Request could not be handled" error appears when configuring SOAP

Tracking ID	Description
	Web Service connector capabilities instead of a message that indicates the cause of the error.
ACM-54603	The error message displayed in the log file should be more detailed when RSA Governance and Lifecycle cannot be started (acm start) after the avuser password has been changed.
ACM-62079	Total item count mismatch observed under tabs for Approvals and Activities.
ACM-62306	The Entitlement Path under a user's Access tab shows an older account name and not the new, latest collected name.
ACM-62423	Running the "customizeACM.sh -i" script generates a "java.io.IOException" error.
ACM-61693	a v7.0 upgrade on RedHat 5.11 fails due to missing oracleasm.