RSA® Identity Management and Governance

V6.9 Service Pack 1 Patch 22 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

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 IMG 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.

March 2017

Contents

Install a Patch

This section explains how to install a patch on an RSA IMG appliance or a soft-appliance server 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 IMG to be re-deployed. See the *RSA Identity Management and Governance Upgrade Guide 6.9 Service Pack 1* for instructions.
- WebSphere: After you deploy the patch, you must restart RSA Identity Management and Governance. When you start RSA Identity Management and Governance after applying the patch, SQL processing is performed. After SQL processing is complete, restart RSA Identity Management and Governance again, to ensure that any patch processing takes effect. To stop and restart RSA Identity Management and Governance 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 Management and Governance.
  4. After the aveksa application has been stopped, click Start to start RSA Identity Management and Governance.

- JBoss: The patch contains a deployment script, patch.sh, to install the patch. See the instructions below.

- TLS 1.1 Support: AFX and some endpoints, such as Salesforce, require TLS 1.1 for connection. As part of the patch, you must download and install an upgrade to the JDK that provides TLS 1.1 support. See the instructions below.

  Note: If you have upgraded the JDK as part of a previous IMG patch, you do not need to upgrade it again.

- 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 Patch

Use this procedure to install the 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 upgrade.

Procedure

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

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

2. Download the upgrade files.

   a. Go to RSA Link, then click Log In and enter your user name and password.

   b. Click RSA Identity Management and Governance.

   c. Click Downloads > Identity Management & Governance 6.9.

   d. Click on Additional Downloads.

   e. Click the Upgrade link for your licensed RSA Identity Management and Governance asset.

   f. Click Download Software.

   g. On the Order Detail page, click the menu icon and select Product List.

   h. Click the Archive tab, then click IMG Access Certification Manager Version 6.9.1P18.

   i. Download the following files:

   - Aveksa_<VersionNumber>_P<PatchNumber>.tar.gz
   - upgradeJDK.tar (mandatory JDK update required for TLS 1.1 support)

3. If you have not already upgraded the JDK, install the upgrade:

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

b. Uncompress and untar the file: `tar vxf upgradeJDK.tar`

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

i. `cd /home/oracle/upgradeJDK`

ii. `chmod 777 *`

iii. `cd deploy/`

iv. `chmod 777 *`

v. cd ..

vi. `sh upgradeJDK.sh`

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

a. `cd /home/oracle`

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

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

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

b. `sh patch.sh`

6. When the patch script completes, restart RSA IMG. Run the following command:

`acm restart`

Download and Import AFX Connector Packages

Use this procedure to download and import the AFX connector package. Reference the instructions in Step 2 above for accessing the software from on RSA Link. In this case, look for an AFX link from Additional Downloads.

Procedure

1. Download the following 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
2. Log on to RSA IMG.

3. Click AFX > Import.
4. Import the packages.
5. Run the following command:

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

RSA Identity Management and Governance

RSA Identity Management and Governance (RSA IMG) offers a comprehensive, business-driven approach to efficiently delivering appropriate access to applications and data resources, whether on-premise or in the cloud.

- Access governance - Governs who has access to what applications and data resources based on job requirements and organization-wide security policies.
- Automated provisioning - Delivers efficient and compliant access changes with rapid application on-boarding.
- Compliance - Ensures that all users in your organization have appropriate access to application and data resources, meeting security and compliance guidelines.

Release 6.9.1 Updates

Version	Date	Description
6.9.1 Patch 22	March 2017	Hotfix Release
6.9.1 Patch 21	January 2017	Patch Release
6.9.1 Patch 20	January 2017	Patch Release
6.9.1 Patch 19	December 2016	Patch Release
6.9.1 Patch 18	September 2016	Patch Release
6.9.1 Patch 17	August 2016	Patch Release
6.9.1 Patch 16	July 2016	Patch Release
6.9.1 Patch 15	June 2016	Patch Release
6.9.1 Patch 14	May 2016	Patch Release
6.9.1 Patch 13	April 2016	Patch Release
6.9.1 Patch 12	March 2016	Patch Release
6.9.1 Patch 11	February 2016	Patch Release
6.9.1 Patch 10	January 2016	Patch Release
6.9.1 Patch 9	December 2015	Patch Release
6.9.1 Patch 8	November 2015	Patch Release

Version	Date	Description
6.9.1 Patch 7	October 2015	Patch Release
6.9.1 Patch 6	September 2015	Patch Release
6.9.1 Patch 5	August 2015	Patch Release
6.9.1 Patch 4	July 2015	Patch Release
6.9.1 Patch 3	June 2015	Patch Release
6.9.1 Patch 2	May 2015	Patch Release
6.9.1 Patch 1	April 2015	Patch Release
6.9.1	March 2015	Service Pack Release

Release 6.9.1 Patch 22

Information about the 6.9.1 Patch 22 release is included in the following sections:

Fixed Issues in 6.9 SP1 Patch 22

Tracking ID	Description
SF-814796, SF-840524, SF-817772, SF-804825 ACM-67872	When a change request is not successfully submitted, pending accounts remain in the system until manually cleaned up.
SF-856733 ACM-68359	Creating a new report that grants a user entitlements to run and view reports erroneously causes previous users to lose those entitlements.
SF-862232 ACM-70364	When an application and rule set have the same name, the account mapping gets rejected while resolving application references, because the name resolves to the rule set.
SF-811933 ACM-64492	Group membership is not displayed under **Users** > **Me** > **What Access** > **Account** > **Groups**.
SF-820993 ACM-65054	In Group Reviews, when signing off a deleted group item, a null pointer exception occurs.
SF-792647 SF-836164 ACM-65704	Role status remains in Applied or Applied New State, even after change request is complete.
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-879935	Performance improvements were made to Multi-Application Entitlement Data Collection.

Tracking ID	Description
ACM-69869	
SF-825742 SF-768664 ACM-62539	When adding entitlements to users, some account template forms are not displayed.
SF-825742 SF-768664 ACM-68221	When adding entitlements to users, some account template forms are not displayed.
SF-914240 ACM-72323	When logged into RSA Identity Management and Governance as a group owner, clicking on the Group tab for a user occasionally results in an error.

Release 6.9.1 Patch 21

Information about the 6.9.1 Patch 21 release is included in the following sections:

What's New in 6.9 SP1 Patch 21

This section lists the features/enhancements introduced in this release.

Feature	What's New
Workflow	Upgraded the Workflow Architect to WorkPoint 3.5.2 Patch 10.

Fixed Issues in 6.9 SP1 Patch 21

Tracking ID	Description
SF-827938 ACM-66135	When a provisioning-termination rule is triggered after identity data unification, it fails to detect some terminated users.
SF-837404 ACM-67489	When selecting Home > Manage Access to view request details, the details page does not show the breadcrumb link properly.
SF-852928 ACM-68053	Patch does not properly migrate workflow jobs which results in display of null instead of count of workflow jobs for the review escalations.
SF-835512 SF-831117 ACM-66909	Collector REQUIRES_FULL_REFRESH values not working as expected in 6.9.1.
SF-861544 ACM-68868	In a workflow transition line, entering more than 64 characters generates an exception error
SF-835031 ACM-66624	User entitlement attribute value is not displaying in the Separation of Duties rule violation tab, after the rule is processed.

Tracking ID	Description
SF-851870 ACM-67724	A view table is missing the expiration date column, forcing users to look elsewhere for the information.
SF-867169 ACM-69593	An SQL table rendered an error when it encountered an incorrect alphabetic character instead of a numeric one.
SF-875454 ACM-69612	A review generation is stuck on a certain step due to performance issues caused by the STG table.
SF-848885 ACM-67482	Technical roles that were previously deleted are reappearing upon migration in Production.
SF-822954 ACM-65328	In SOAP and REST Nodes, embedded variables are not being substituted correctly and are sent as null.
SF-635834, SF-679132 ACM-53637	Using an advanced search filter with multiple parameters returns an error.
SF-746543 ACM-63437	During account creation, when AFX reports a failure due to a duplicate user, the associated change request reports a success.
SF-855812 ACM-68176	Disabled accounts collected using the Lotus Notes collector are incorrectly displayed as active.
SF-890199 ACM-70598	The size of the T_AV_ROLE_METRICS table is growing at a dramatic rate.
SF-843099 ACM-67381	The Active Directory ADC is unable to collect group memberships for accounts with DNs longer than 256 characters.
SF-893870 ACM-70786	If an account has been deleted before a Change Request item has been fulfilled, upon completion of fulfillment node a null pointer exception occurs.
SF-825171 ACM-69369	When a member is deleted from a local role and then added again, duplicate entries for that member are created in the T_AV_ROLEMEMBERSHIPS table.

Tracking ID	Description
SF-00736035 ACM-58035	When attempting to add entitlements to a user with multiple accounts, the account is incorrectly displayed as Disabled = False
SF-737360 ACM-57480	The Active Directory ADC is unable to map the group owner to a user attribute that is longer than 256 characters.

Release 6.9.1 Patch 20

Issues fixed in the 6.9.1 Patch 20 release are described in the following section.

Fixed Issues in 6.9 SP1 Patch 20

Tracking ID	Description
SF-835268 ACM-66722	When creating an account using the Active Directory connector, the connector does not accept more than 26 parameters.
SF-810184 SF-820915 SF-842422 ACM-66623	Creating an account with an initial password (using the Active Directory connector) fails because password is not accepted.
SF-832126 ACM-66514	Role Definition review result lists "deleted" and "terminated" users.
SF-810120 ACM-64976	When running a User Access review with the Include sub-groups option checked under Content, no users who are members of the selected group are included in the review.
SF-814121 ACM-64423	A duplicate user is created after moving the user from a collector with lower priority to another with higher priority in a data unification configuration.
SF-865617 SF-858097 ACM-68704	An " ORA-30926: unable to get a stable set of rows in the source tables" error occurs when attempting to modify a role.
SF-859156 ACM-69165	In a Request Form, when the control type is set to Entitlement Table and the "Select only one entitlement" option is selected, the form still allows a user to select multiple entitlements.
SF-827134 ACM-65820	Count reported in review status message does not match items selected in the review.
SF-815249 SF-787876 SF-808059 SF-823486 SF-812840	When a change request that includes creating an account is created by a Role rule, the request creates a pending account with the wrong account name.

Tracking ID	Description
SF-835037 SF-867034 SF-851571 ACM-65010	
SF-858765 ACM-68800	The Reject button is missing in a change request Approval form.
SF-00818519 SF-00868378 ACM-64853	A script within version 6.9.1. generates an error that the upgradeJDK.tar file is not supported on Linux RedHat.
SF-00841751 ACM-67014	An unnecessary check for an OS generated an error when attempting to upgrade the JDK patch.
SF-760015 ACM-68215	System performance was degraded and the following error was observed: "Error reading request, ignored java.lang.OutOfMemoryError: Java heap space."

Release 6.9.1 Patch 19

Information about the 6.9.1 Patch 19 release is included in the following sections:

Fixed Issues in 6.9 SP1 Patch 19

Tracking ID	Description
SF-799626, 831906 ACM-63141	A user is unable to use Shift-Click to select a range of table items.
SF-768662 ACM-62557	Not all information questions provided in a request form are displayed to a user who is requesting access.
SF-764664 ACM-61365	A change request is not generated when a remediator revokes an SoD or user access rule violation entitlement.
SF-81656, 834552 ACM-64937	A review took a considerable longer amount of time to complete in a production environment after an upgrade to 6.9.1p10.
SF-747182, 825742 ACM-58834	When requesting access, clicking the submit request button, and then clicking Cancel results, accounts with a placeholder value are created in the database and shown under the user.
SF-844480, 843836 ACM-67253	Unable to submit change requests or complete existing workflows.
SF-841932 ACM-67259	The selected user in a request form is lost if the user has multiple first or last names.
SF-805551 ACM-63789	A review's "Due By" column displays "null days left."
SF-802638, SF-797279, SF-789403 ACM-64929	Requests will not pass the verification stage even though watches are completed and changes are collected, which prevents Workflows from progressing.

Tracking ID	Description
SF-825567 ACM-66659	Only the prefix for a change request is displayed in the Requests window when the workflow that initiates the request for a Provisioning-Termination rule violation is configured with that prefix.
SF-799755 ACM-63214	In a Request Form, conditions may not behave as expected due to incorrect unicode/UTF-8 handling in dependent field values that contain unicode characters.
ACM-65578	When a form with the Display option enabled is run, the User Account Table does not load accounts and displays a count of 0.
SF-799702 ACM-67147	Create account change items for indirect entitlements are not rejected when the related direct entitlement (role) is rejected in a change request.
SF-00820125 ACM-64971	An escalation email created from each job approval contains a list of all users affected by the main Change Request, instead of just the affected user.
SF-840381 ACM-67302	The system is inoperable because of a "Unable to start service ChangeRequestService" error, which is precipitated by a "ORA-01403 in UTILITIES_PKG" error.
SF-824730 ACM-66406	A performance issue is observed with Admin > Email > Log.
SF-841202 ACM-67681	A performance issue is observed with My Tasks > My Reviews.
SF-847001 ACM-67378	Application crashes and aveksaServer.log shows "too many open files" error.
SF-775070 ACM-63936	Rule violation remediator assignment missing for user access and segregation of duties rules.
SF-00853427 SF-00849624 ACM-67871	Authentication fails if the authentication source uses an Account Data Collector and the AccountSearchAttribute is different than the distinguishedName (used as the Account Name).
SF-861720, SF-871676, SF-877268 ACM-68574	When configuring an account collector to collect groups to sub-groups membership, the resolution fails and the sub groups are collected with type "Account" under the "Member Type" field.

Release 6.9.1 Patch 18

Information about the 6.9.1 Patch 18 release is included in the following sections:

What's New in 6.9 SP1 Patch 18

This section lists the features/enhancements introduced in this release.

Feature	What's New
AFX Server	Improved logging of an RSA IMG response when it cannnot be parsed (not in expected XML format).
Connectors	Improved the performance of the Create/Edit Connector page by loading only the properties needed to render the page.
Access Request Forms	To improve security of request forms, the Create New Form, General Properties now includes an "Availability" filter. This filter sets who can use the form to create a request. To run any type of form, the user must have one of the following types of access: • Included by the Availability setting • System administrator • Access Request Administrator entitlement

Fixed Issues in 6.9 SP1 Patch 18

Tracking ID	Description
SF-826482 ACM-65590	The Long Description is not applied correctly for an object after a metadata file import and the description filter contains an underscore (_) character.
SF-813931 ACM-64726	The following error related to a multi-app entitlement collection is observed in system logs: "ORA-12899: value too large for column."
SF-773829, 818058 ACM-64376	Identity collection from an LDAP source fails with multiple Oracle errors.

Tracking ID	Description
SF-616653 ACM-51924	Page 3 in an entitlement collector definition takes an inordinate amount of time to load.
SF-819325, 818430 ACM-65126	Users who match a role membership rule criteria do not match the criteria after they are removed from the role.
SF-829214 ACM-65981	In an Approval node in a workflow, when using a group to review changes, using more than 10 members in the group resulted in an error when a change request is submitted.
SF-828015 ACM-65761	Non-privileged user can edit AFX connector and change the capabilities.
SF-802279 ACM-63383	Invalid characters within a XML CLOB prevents data runs after migration.
SF-727740 ACM-56696	When a user completes an Access Request form, a validation error displays and not all values are correctly returned.
SF-740736 ACM-59192	When upgrading from 6.9.1 P06 to P07, entitlement data collectors are unable to complete the collection process.
SF-792922 ACM-63524	Accounts were enabled multiple times.
SF-780279 ACM-61688	The following error occurs when running a user access review: "ORA-20126: The creation of reviews failed. Stored Procedure:Parse_Roles_In_User_Review execution aborted. ORA-01427: single-row subquery returns more than one row."
SF-784859, 735335, 740094 ACM-64624	A user is granted a duplicate role when the role has a custom attribute value.
SF-800603 ACM-63666	Rule creation with an Advanced condition expression fails.
SF-828448 ACM-65814	Connector password mapping strips password containing certain special characters.

Tracking ID	Description
SF-824709 ACM-65504	AveksaAgent and AFX become unresponsive in a high network usage scenario.
SF-825335 ACM-65610	A non-privileged user can generate a change request by changing the OID value in the change request URL.
SF-828016 ACM-65765	A non-privileged user can edit Attribute Synchronization settings.
SF-627462 ACM-52588	A change request generated for a user who has an account revoked in an account access and ownership review does not appear in the user's Requests tab.
SF-804825 ACM-63833	Change Requests for entitlements are not created with the necessary Create Account items for those entitlements.
SF-799626 ACM-63141	A user is unable to use Shift-Click to select a range of table items.
SF-768662 ACM-62557	Not all information questions provided in a request form are displayed to a user who is requesting access.
SF-769981, 780942 ACM-60837	Accounts created from an account template are not removed from the user interface when the request item is rejected and canceled.

Release 6.9.1 Patch 17

Information about the 6.9.1 Patch 17 release is included in the following sections:

What's New in 6.9 SP1 Patch 17

This section lists the features/enhancements introduced in this release.

Feature	What's New
Connectors	The default timeout value for an SSH connector has been increased to 60 seconds.
Reviews	The Generate Change Request configuration option is fully supported for the Data Resource Access and Data Resource Ownership review types.
SSO for Web Services	Added support for Single Sign-On (SSO) to authenticate users of RSA IMG Web Services.
Web Services	The updateReviewItems command enables you to update one or more items in a user access review that is in an actionable state. See the command's description in Admin > Web Services for instructions on how to use the command.

Fixed Issues in 6.9 SP1 Patch 17

Tracking ID	Description
SF-797159 ACM-63406	Web services does not include a command to take action on particular user access review items. See What's New in 6.9 SP1 Patch 17 for information on the new updateReviewItems command.
SF-792326 ACM-62771	An account data collection from an LDAP source does not complete processing due to a time out error.
SF-775755 ACM-61928	Required entitlement field in Access Request form is empty, but form is still submitted.
SF-812781	Under a user's Access tab, an entitlement indirectly granted to the user through

Tracking ID	Description
ACM-64290	membership in role does not indicate that the entitlement belongs to the role.
SF-797168 ACM-64217	The Overall Status bar on Request status does not show completed (100 % green) when the change request is forced to complete. This issue was fixed so that the Mark Verified node gets the Request Form item
SF-795918 ACM-62913	Access Request form displays L2 and L3 approvers that have been removed from the application roles.
SF-795519, 822221 ACM-64496	Office 365 Account Data Collector (ADC) does not collect accounts properly when more than 500 accounts.
SF-812262 ACM-64497	In a workflow, an Approval node is disconnected from the Approvals phase when using Group By Role Owner.
SF-792313 ACM-63539	Authorization bypass to product features is observed.
SF-799174 ACM-63105	Slow page load observed in the Requests > Activities > By Entitlement page from a monitoring policy view.
SF-820237, 811129 ACM-65049	A directory reference ID is incorrect after an XML file export.
SF-760015,784081 ACM-60459 ACM-64559	Slow performance experienced with the system. In Requests> Activities, accessing "ActivityByBusinessSourceTable" results in long-running process.
SF-775070 ACM-64374	Inability to close a rule remediation task even though all violations for that task have already been remediated in other tasks.
SF-838478 ACM-66673	An "IndexOutOfBoundsException" error occurs when clicking on the "Form" tab in any activity node having less than two outbound request-button transitions.
SF-799972 ACM-63350	Account review generation fails when using Turkish (double-byte) characters in the display name.
SF-815444	Password change emails queued with no justification.

Tracking ID	Description
SF-826425 ACM-64605	

Release 6.9.1 Patch 16

Information about the 6.9.1 Patch 16 release is included in the following sections:

What's New in 6.9 SP1 Patch 16

This section lists the features/enhancements introduced in this release.

Feature	What's New
Collectors	The following configuration options are available for collectors that collect from Active Directory and LDAP data sources: • Connection Timeout: It enables you to specify the time in milliseconds a collector waits to complete the initial TCP connection handshake before the connection attempt is aborted. • Read Timeout: It enables you to specify the time in milliseconds a collector waits to read data after the previous read before the read attempt is aborted. These options enable you to ensure that a collection does not remain in a stalled state if connection or read operations are hindered by a slow network.
Connector Templates	Improved overall performance (rendering, searching, sorting) of the AFX > Connector Templates page.

Fixed Issues in 6.9 SP1 Patch 16

Tracking ID	Description
SF-792371, 797976, 815955 ACM-62549	Change verification after account collection takes over 14 hours to complete.
SF-812801 ACM-64291	The Remove action is available for a group entitlement indirectly granted through a role under the Access tab for a user who has the role.

Tracking ID	Description
SF-762287 ACM-60751 ACM-62504	When a user is a member of a business role that has a technical role as an entitlement, the user is granted the technical role twice, a direct entitlement and an indirect entitlement.
SF-792006 ACM-63562	In an account access and ownership review, the group by Account User filter does not work.
SF-808921 ACM-63946	Unification has been running an inordinate amount of time.
SF-784081 ACM-64480	A performance issue is experienced with the SecurityContext.csv query.
SF-798406 ACM-63215	All requests for a particular application are auto canceling.
SF-730437, 808076 ACM-57967	After updating MySQL driver to v5.6, an account data collector test fails with a SQL syntax error.
SF-804303 ACM-63641	A completed request is incorrectly indicated as in the fulfillment phase in the Request Details screen.
SF-813763 816920, 818290 ACM-64568	A "Parsing failed at line" error occurred during a rule membership configuration operation for a role.
SF-806147, SF-806198 ACM-63935	AFX requests that fail to fulfill at the target system get stuck and do not create manual activities (in AFX fulfillment workflows) or move to the next workflow node (when provisioning command nodes). This issue was fixed by accounting properly for unicode characters.
SF-814060 ACM-64663	When completing an access request form, a warning prevents the user from saving an advanced mode query because it cannot be represented in basic mode

Release 6.9.1 Patch 15

Information about the 6.9.1 Patch 15 release is included in the following sections:

What's New in 6.9 SP1 Patch 15

This section lists the features/enhancements introduced in this release.

Feature	What's New
Attributes	You can create a custom value list for attributes of the integer data type. The General and the Value tabs have been removed. All configuration options are consolidated in the Create Custom Value window.
Collectors	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	The Salesforce connector supports API v36.0. The Generic REST connector supports HTTPS connection to a Zendesk endpoint.
Email	The following JavaMail email configuration settings are included under Admin > Email > Settings: • Mail connection timeout: The socket connection timeout value in seconds. The default value is 180 seconds. • Mail timeout: The socket input/output timeout value in seconds. The default value is 180 seconds. • Mail writer timeout: The socket write timeout value in seconds. The default value is 180 seconds.
Web Services	The createChangeRequest command includes the "Terminate User" operation. .
Workflow	The option to reset the job was removed from the Job menu in

Feature	What's New
	workflows.

Fixed Issues in 6.9 SP1 Patch 15

Tracking ID	Description
SF-752280 ACM-60146	When adding users from RSA IMG through a join request into an identity source, users with an apostrophe in their name get a double apostrophe.
SF-784527 ACM-62533	Selecting the 'Account Creation Date' system attribute 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-793943 ACM-62896	The Active Directory identity data collector is not able to collect users through encrypted and non-encrypted LDAP servers.
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-791875 ACM-62506	When selected user does not populate any accounts into the table, the "User Account Table" field, in the request forms, returns a "required" warning, even though it is not configured as a required field.
SF-785022 ACM-62505	User review shows the direct membership of nested roles.
SF-779202; SF-773511 ACM-62921	When using SSL with the generic SOAP Web Services Connector, AFX ignores any certificates in the default truststore or any keystore paths specified in the UI connector configurations.
SF-780836 ACM-61537	An entitlement data collector takes an inordinate amount of time to collect entitlements.
SF-772835 ACM-61667	Role collections takes three hours to complete.
SF-793954	A workflow statement fails with an 'Invalid column index' error.

Tracking ID	Description
ACM-62731	
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-797586 ACM-63054	Unable to export a report after applying 6.9.1 patch 12.
SF-796876 ACM-62980	Terminated users cannot be selected from a user selection picker in a request form even though the form is configured to allow selection of terminated users.
SF-802569 ACM-63890	When activities are filtered by the "By Assignee" tab, activities are duplicated as many times as the number of tasks that are in the activity.
SF-738151 ACM-56484	Salesforce.com AFX Connector is not working with Salesforce API 34.0 to create an account for Salesforce.
SF-762176 ACM-60865	Patch installation fails if an "admin" account does not exist.
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-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-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.
Lotus Notes ACM-61775	The Lotus Notes entitlement collector does not support collection of a replica IDs. See What's New in 6.9 SP1 Patch 15 for more information.
SF-813273 ACM-64373	Performance issue observed closing watches in requests due to large-sized requests and inefficient processing of JMS events.
SF-783226,	Several user interface elements are "grayed out" when using Internet Explorer

Tracking ID	Description
803077 ACM-62595 ACM-65223	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.
SF-767203 ACM-63649	A requestor is experiencing delays in navigating through the change request procedure when requesting access to a role.

Release 6.9.1 Patch 14

Information about the 6.9.1 Patch 14 release is included in the following sections:

What's New in 6.9 SP1 Patch 14

This section lists the features/enhancements introduced in this release.

Feature	What's New
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. This reduces the chance of a timeout occurring while AFX is waiting for a response from RSA IMG.
Collectors	The Lotus Notes Entitlement Data Collector has been upgraded to: • Collect all application filenames • Collect Application title • Collect Potential Entitlements • Collect Actual Entitlements
OpenJDK	Some endpoints, such as Salesforce, require TLS 1.1 for connection. As part of the patch, you have the option to download and install an upgrade to JDK that provides TLS 1.1 support. For instructions, see the Install a Patch topic.
Workflows	Only workflow work item history is accumulated. This prevents unnecessary accumulation of workflow data in the database

Fixed Issues in 6.9 SP1 Patch 14

Tracking ID	Description
SF-777489 ACM-61686	After upgrading from 6.8.1 P20 to P22, a "The request could not be handled" error appears under the General tab when a user attempts to edit or create new reports.
SF-792013	When a bind variable is added to a report, the resulting exported CSV report result

Tracking ID	Description
ACM-62488	file is blank.
SF-711897 ACM-55731	AFX connectors do not install when imported from a development environment to a test environment in WebSphere v8.5.
SF-783596 ACM-61770	Leaking CLOBs and XMLType exceeded maximum temporary space over a period of time.
SF-620305 ACM-52017	Terminating a user using the Default Terminate Form accessed from a request button 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-746921 ACM-58879	Cancelling change requests that are in the Open state does not roll back role changes.
SF-760448 ACM-60355	Scheduled backups are not executing automatically.
SF-740094, SF-740342 ACM-61117	Based on the number of remediators, duplicate work items are displayed under the Violation Remediation tab.
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-632425 ACM-52120	SQL injection threat observed when importing a workflow.
SF-660715 ACM-53471	Lotus Notes Entitlement Data Collector has been enhanced to increase collection efficiency.
SF-803677 ACM-63495	Workflow stays in the Created state until it is manually evaluated.
SF-770400; SF-756694	MAL: The connection to remote agents timeout, interrupting the collection process.

Tracking ID	Description
ACM-60732	
ACM-62646	Resource leak from the ojdbc driver. The ojdbc driver used to configure the ACM Oracle JDBC Driver needs to be updated. 1. In Websphere, confirm the Classpath used for ACM Oracle JDBC Driver and the ACM Oracle JDBC XA driver 2. In Websphere console: Resources >JDBC >JDBC Providers > choose the provider 3. Look at the Class Path under general properties. 4. If it uses a variable for the class path (ie. ORACLE_JDBC_DRIVER_PATH) identify the full path by looking up the variable: Environment >Webpshere variables page. 5. Once you have identified where the currently configured ojdbc5.jar file is configured, back up the existing one and copy the one supplied in the Patch tar file. 6. Restart the WebSphere server.

Release 6.9.1 Patch 13

Information about the 6.9.1 Patch 13 release is included in the following sections:

What's New in 6.9 SP1 Patch 13

This section lists the features/enhancements introduced in this release.

Feature	What's New
Attributes Detail URL	User-created attributes now support Detail URL feature so the end-user can see information about an attribute outside of what is collected and managed in RSA IMG. For example, end-users may want additional information about a specific collected entitlement or group. You can add an attribute Detail URL so that when an end-user clicks on the information icon for that entitlement or group attribute, they are directed to the central repository website for information. The attribute Detail URL is located under: Admin > Attributes > Edit in the selected object tab. To create the URL, use the following format: http://<URL of the website> Detail URL also incorporates variable substitution, where you add a variable to the URL to pass an ID from one attribute to another. To add the variable substitution to the URL: Enter the URL, click the drop-down button, and select an object attribute value from the drop-down. To create a URL with variable substitution, use the following format: http://<URL of the website>?id=${<Attribute name>} **Note:** This is feature available for all user-created attributes. The URL external links must have a matching resource IDs to enable RSA Governance and Lifecycle to connect to the web application.
Patch Documentation	Patch_README.txt has been removed and the content is now included with the Installing a Patch documentation.

Feature	What's New
Workflows	The workflow engine was upgraded to resolve issues such as: • Processing queue items. • Null pointer exceptions when reading from the JMS queue.

Fixed Issues in 6.9 SP1 Patch 13

Tracking ID	Description
SF-758811 ACM-60041	SOAP connector fails with a NullPointerException.
SF-745588 ACM-60984	The user using the REST Web Services node is unable to set "Content-Type," which instead defaults to "text/plain."
SF-664646 ACM-53395	"On Hold" reviews appear as pending actions on reviewer's homepage rather than just the "Active" reviews.
SF-750619 ACM-60722	When the monitor tries to access a review using the hyperlink created from the variable review_rvw_url, an insufficient privilege error appears.
SF-697502 ACM-55009	When the reviewer reassigned a review item to other reviewers without giving them the sign-off privileges to delegate, the review item is not removed from the former reviewer's list, even if "Remove selected items from my review" function is selected.
SF-777907 ACM-61295	When filtering business sources in any review definition, using an SQL statement with new lines in 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-780558 ACM-61585	On the Account Selection page, LAST_LOGIN_DATE attribute is not displayed in the Filter accounts section.
SF-751445 ACM-60780	When the user attempts to view the Entitlement tab under Activities page, the stack overflow error is observed in the user interface.
SF-771705	In a multi-step user access review, when the first step is not generated, the second

Tracking ID	Description
ACM-61364	step review generation fails with unique constraint error.
SF-782388 ACM-61635	An "ORA-01000: maximum open cursors exceeded" error occurred when a report was generated.
SF-650965 ACM-53908	When configuring the REST Web Services Connector, the Command Code Path input field cuts off all of the content after "&".
SF-783309, 766351 ACM-61786	The "Security Token" field appears as mandatory in the SalesForce Data Collector configurations.
SF-742255 ACM-61399	Provisioning Joiner/Mover rule is not successfully adding all of the users from RSA IMG to Active Directory.
SF-713802 ACM-55974	A Long Description hyperlink does not open in a new window/tab, rather the current window is replaced by the hyperlink URL.
SF-749705, 757128 ACM-58548	The server takes an long time to start and migrate the .jrxml files.
SF-775070 ACM-60987	Unable to assign remediators to unassigned rule violations.
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-785372 ACM-62204	A terminated and then re-hired user does not match the previous membership rule for the past role.
SF-773609 ACM-60921	RSA IMG is not displaying dashboards according to the display sequence.
SF-777383 ACM-61303	In some dialog boxes, non-privileged users can access other user's data.
SF-792013 ACM-62488	When the user added a bind variable to the report, the resulting exported CSV file was blank.
SF-758596	After the customer rebuilt a collector, they could no longer submit requests for

Tracking ID	Description
ACM-59675	their roles.
SF-783876 ACM-61754	The Retention value under the System Log tab shows a string variable instead of a number.
SF-787727 ACM-62247	The report was not imported properly, resulting in the bind variables Default Values not appearing on the query page of the report.
SF-739306 ACM-57618	JavaCodeBased Connector cannot be saved once its re-uploaded. after deletion.
SF-792812 ACM-62643	The Entitlement Data Collector does not work with a custom database driver after the upgrade.
SF-796872 ACM-62981	The Entitlement Name field is not required when creating a request form for a new group access for UNIX platform.
SF-789930 ACM-62400	Business description processing taking 30 minutes to process 168,000 records.

Release 6.9.1 Patch 12

Information about the 6.9.1 Patch 12 release is included in the following sections:

What's New in 6.9 SP1 Patch 12

This section lists the features/enhancements introduced in this release.

Feature	What's New
Custom Attributes	When working with the "application" object in custom attributes (Admin > Attributes > Custom List), a third option, Name, was added to allow for use of a "friendly" name, in addition to the Raw name.
Form Controls	This patch release introduces a multi-select drop down control that presents a list of options that the requestor can select. The value for the selected options will be stored in the associated workflow variable.
Request Forms	Provides users the ability to access the request form from an external website or portal. See Accessing External Request Forms from an External Portal in the Documentation Supplement.
CyberArk Guide	This patch release introduces the CyberArk Application Guide for working with the CyberArk collectors and connectors. Refer to RSA Link- RSA Governance and Lifecycle to download the guide.
Data Collectors	See new information about port usage for LDAP searches from a Global Catalog in Configuring Access to a Data Source in the Documentation Supplement.

Fixed Issues in 6.9 SP1 Patch 12

Tracking ID	Description
SF-751426 ACM-60715	The specified parameter for 'Maximum repeated characters' in a password policy does not save after the user changes it.

Tracking ID	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-719853 ACM-56512	The system updates the database with partial read results after an LDAP collection when a search operation is abandoned or terminated.
SF-689578 ACM-54594	Running the modifyhostname.sh script on V6.9.1 fails with a " /usr/bin/modifyhostname.sh: line 157: ../acmcerts.sh: No such file or directory" error.
SF-754154, 771853 ACM-59329	Cannot collect from a cloud-based Workday application without the ability to define web proxy.
SF-596695, 743574 ACM-50656	WebSphere logs the following message "There are currently 100 open JMS Producers for the Session." This has been fixed so that the application closes producers that are not required.
SF-749898 ACM-58642	AFX download server delivers a zero size file when there is not enough space user /tmp. This error was indicated in the log file, and is now also shown in the user interface.
SF-775551 ACM-61215	Submission variable is not appearing on all Change Requests, when the change request uses a custom form with grouping by user and multiple users are submitted. This issue has been fixed so the variable now appears on the Change Request for each user.
SF-759424 ACM-59853	Workday Identity Collector fails with an error "Failed to add WS-Security header to request"
SF-762063 ACM-59782	Extra AFXPlugIntemp_connector_migrationafx-connector files appeared in the WEB-INF/plugins directory.
SF-676846 ACM-54817	The 'Overall Status' in a review result refreshes automatically to update the displayed time and date even after the completion of the review.
SF-684046 ACM-54433	Values for a drop down control in request forms cannot be deleted if the value contains quotes.
SF-721068 ACM-56878	A large report with over 65,000 lines could not be exported as a usable file. There is limit of 1048576 records that can be exported to an Excel spreadsheet.

Tracking ID	Description
SF-748387 ACM-58768	Previously, the user could only enter a valid email address in the user selection pop-up in order to filter users by their email id. Now if filter operator says "contains", "does not contain", "matches", "does not match", "one of", and "not one of" in Simple search, then the user can search the non-empty string keyword to filter users by their email id. This function is applicable to all user selection pop-ups.
SF-780558 ACM-61585	On the Account Selection page, the LAST_LOGIN_DATE attribute is not displayed in the Filter accounts section.
SF-751445 ACM-60780	When the user attempts to view the Entitlement tab under Activities page, the user interface generates a stack overflow error.
SF-758073 ACM-59428	The entitlement collector fails during the database processing stage.
SF-779987, 781181 ACM-61431	When the customers runs the SQL query, no output is received and only the message "PL/SQL successfully completed" appears.
SF-760264 ACM-60527	Test Connection for Soap Connector to Lync AFX fail.
SF-782388 ACM-61635	An "ORA-01000: maximum open cursors exceeded" error occurred when a report was generated.

Release 6.9.1 Patch 11

Information about the 6.9.1 Patch 11 release is included in the following sections:

What's New in 6.9 SP1 Patch 11

This section lists the features/enhancements introduced in this release.

Feature	What's New
Aveksa Statistics Report	Updated the Statistics Report to include workflow history and AFX connector information.
Workflow	A new request source is included under Requests > Workflow > Overview: "Request created through web services will be processed using *[Request workflow]*".
Database	The V_CHANGE_REQUEST_DETAILS database view has been deprecated. It no longer serves the purpose it was originally designed for, and input/output operations with the table degraded system performance.

Fixed Issues in 6.9 SP1 Patch 11

Tracking ID	Description
SF-709543 ACM-55802	When Change request initiates via Roles, the Account Changes table shows 'Error' message.
SF-721255, SF-719473, SF-735339, SF-635183 ACM-52583	Fulfillment activities are listed under the approval header in change request.
SF- 754270 ACM-59469	When supervisor rejects a user's entitlement, other user's entitlements are also rejected.
SF-730477	Null pointer exceptions occur when a workflow process is not found.

Tracking ID	Description
ACM-56763	
SF-744512 ACM-57938	Review generation is very slow after the migration from version 6.8.1 P11 to 6.8.1 P21.
SF-615695 ACM-51519	Attribute change rule does not work with Unique ID condition using contains/not contains operator.
SF-748712 ACM-58549	The reported reviewer is wrong for the reviews that use the alternate reviewer coverage file.
SF-741373 ACM-57697	Scheduled reports send an e-mail without an attachment when the option "Delete the report result after sending e-mail" is checked.
SF-762350 ACM-59820	The workflow gets an error at the Workflow Path and stops.
SF-763467 ACM-60229	A user with a "Directory: Admin" entitlement is not able to edit Groups.
SF-760264 ACM-60527	Test Connection for Soap Connector to Lync AFX fail.
SF-: 717985, 750682 ACM-58936 ACM-57316	An "Illegal TXN state" error occurs when a user task is invoked from the My Tasks menu.
SF-757199 ACM-60655	When the option "Allow monitors to update their review metrics" is unchecked, it cannot be saved.
SF-696357 ACM-54978	Unable to run "Change Request Status Summary, by day for past month" Access Request report.
SF-763404 ACM-59907	A change request to commit changes to a role takes an inordinate amount of time to complete.
SF-772393 ACM-61086	An account review is completed but the Completed Status bar indicates that it is not completed.
SF-777383	Specially constructed URLs could allow information leakage vulnerabilities where

Tracking ID	Description
ACM-61303	a user could view information for which they do not have privileges. This issue was fixed.

Release 6.9.1 Patch 10

Information about the 6.9.1 Patch 10 release is included in the following sections:

What's New in 6.9 SP1 Patch 10

This section lists the features/enhancements introduced in this release.

Feature	What's New
AFX Administration: Check Owner Permissions	As a security best practice AFX Servers should not be installed and administered as root. AFX should be installed and run in a less-privileged account. A warning is displayed if AFX is installed and run from the root account. Also, if the AFX servers are started from an account that does not have the appropriate owner permissions, a warning is displayed and start-up is prevented.
AFX: Ability to Constrain the Size of Daily Logs	The Daily Logs generated by AFX can use a large amount of disk space. These logs rollover to a backup file on a daily basis. To constrain the amount of space used by these logs, newly generated daily logs will rollover when the file reaches a size of 100MB. The number of backup files is limited to 5 files. New rolled-over logs (files that end in .log.* rather than .log) will change from ending in a date string (e.g. .log-2015-11-18) to ending in a number string (e.g. .log.2).
Change Requests	The following table option columns are available for entitlements in change requests: • Entitlement Short Description • Entitlement Long Description
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.

Feature	What's New
	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" topic in the Documentation Supplement.
Rules	When configuring rules, you can allow common entitlements in a segregation of duties (SoD) rule. For more information, see the "Configure Processing Schedules and Triggers" topic in the topic in the Documentation Supplement.
Statistics Report (formerly the Aveksa Statistics Report)	Updated the Statistics Report to include workflow history. For more information, see the Help topic, "Generate a Statistics Report."
Workflows	In the Manual Fulfillment workflow, within the Fulfillment node, in the Activity properties, on the Form tab, you can now use "Reassignment when more than 0 occurrences" successfully. This provides support for multiple reassignments and a custom escalation workflow.

Fixed Issues in 6.9 SP1 Patch 10

Tracking ID	Description
SF-705079 ACM-55609	Collection time is three times slower after an upgrade from v6.5.2 to v6.9.1.
SF-682323 ACM-57092	When 'Resolve all user references using unique attribute' function uses 'User ID' attribute, the program returns 'General metadata: Import Failed' response to the user.
SF-744510 ACM-57935	The View Report and Run Report settings for an imported report are incorrect.
SF-667254 ACM-54592	The user does not see consistent "Requested on" dates for the same change request.
SF-749192 ACM-58702	Change verification in role collection is executing for an inordinate amount of time.
SF-752247 ACM-58850	Unification is taking an inordinate amount of time to complete because of "Step 7/10- "Populate Role Metrics" taking 54:55 hrs" (from the Statistics Report).

Tracking ID	Description
SF-747182 ACM-58834	When requesting access, clicking the submit request button, and then clicking Cancel results, accounts with a placeholder value are created in the database and shown under the user.
SF-752364 ACM-58996	When creating a role set, in role set policies, the 'Deny members not matching the membership rule' setting is not limiting the users available to select. The setting now limits the users that can be added as members to the scope of the previously selected users.
SF-739768 ACM-57803	AFX connectors had 'Application' mapping attributes populated only for account related capabilities. The mapping attributes have been extended to cover other capabilities.
ACM-58621	SOAP Connector: Not able to configure Output parameter response for CreateAccount capability.
SF-586635 ACM-50956	When a supervisor is chosen in an SQL select node in an escalation workflow, a request is not reassigned after an approval workflow times out.
SF-735050 ACM-57062	A user who is a role member and an other business owner is unable to edit applications and collectors.
SF-724380 ACM-56603	Group description CSV file bulk import not working properly.
SF-651786 ACM-53517	The multi-app account collector is not collecting the 'extensionAttribute' attribute.
SF-724142 ACM-56748	WebService commands collectAccounts and collectEntitlements are inconsistent.
SF-682435 ACM-55751	The system keeps logging errors regarding the failure in executing a JDBC query.
SF-689941 ACM-54588	The user is not able to select Apply Changes in the Edit Entitlements tab.
SF-732155 ACM-56879	The WebService change request is always passed to the request workflow as "Delegated approvals with default."
SF-747689 ACM-58431	The termination rule creates a change request to disable an account that is already disabled.

Tracking ID	Description
SF-740219 ACM-57615	Following an upgrade to v6.8.1 patch 19 from v6.8.1 patch 8, the Requests page and the Workflow page take a long time to load.
SF-669990 ACM-53673	When using the user account table control type for choosing accounts in an access request form, the form does not allow a supervisor to select a subordinate's account. A supervisor can now select the account to create an access request.
SF-765036 ACM-60137	After upgrading to v6.9.1.09, RSA IMG startup fails due to SSO error. This issue has been fixed.
SF-759615 ACM-59522	Role change request is created with wrong requestor.

Release 6.9.1 Patch 9

Information about the 6.9.1 Patch 9 release is included in the following sections:

What's New in 6.9 SP1 Patch 9

This section lists the features/enhancements introduced in this release.

Feature	What's New
Active Directory Wizard: Collector Configuration: Object SIDs	The wizard allows you to process group members that are a Foreign Security Principal (FSP) within Active Directory. This requires each Active Directory collector to collect the object SIDs for accounts and groups. To collect the object SIDs, you must select the Collect ObjectSID option.
Change Requests:Entitlement Descriptions	The following table option columns are available for entitlements in change requests: • Entitlement Short Description • Entitlement Long Description
Drop-down Select with web service	Allows you to display a list of selection options for the requestor. The values for the selected options are loaded at run-time from the URI provided.
Drop-down Select	Displays a list of selection options for the requestor that you specify. Also, you can specify a corresponding value for each selection. This value is set in the variable name for the control, based on the form requestor's selection.
Review Definitions: Entitlement Filtering	The following review definition filters define the scope of business sources for which entitlements are reviewed: • The "Filter business sources" option under the Content tab for user access and account access and ownership review definition types. • The "Selected roles" option under the Role selection tab for the role definition review type All further review definition options for these review types apply only to the business sources defined by the scope.

Feature	What's New
Rules: Testing	The Provisioning - Termination and the Provisioning - Joiner/Mover rule definitions include a Test button.
Rules: SoD	When configuring rules, you can allow common entitlements in a segregation of duties (SoD) rule. For more information, see Configure Processing Schedules and Triggers in the Documentation Supplement.
Web services: Access Requests	Added new functionality to allow an external application to include additional information as part of an access request. In Admin > Web Services > Request Commands, the createChangeRequest command now has a CustomAttribute parameter that can be used to include additional information, and the custom attribute can also be available in the approval and fulfillment processes. To support additional information in these requests, an admin can add custom attributes for change request items (CRI) by going to Admin > Attributes, then selecting the Change Request Items tab. The "CRI" custom attributes follow the same model (String, Date, Integer) types that are available for other attributes. The "CRI" custom attributes are available in the table options for all approval / fulfillment tables. When the activity is sent to fulfillment (and it is automated - AFX), the associated CRI custom attributes are also available.
Workflows: Reassignments	When performing approval or fulfillment activities, you can now reassign your activities to multiple (up to 10) users. This setting can be configured at the activity node level by using the Maximum Users Selectable for Reassignment option. If this setting is greater than 1, the multi-user picker is displayed.
Workflows:Escalations	In a Manual Fulfillment workflow, in an Action node's Activity properties, on the Form tab, the Allow Reassign option did not work with escalations when the Reassignment threshold was set to more than 0 occurrences. This option was not firing escalations when more then 0 reassignments occur. Now, an escalation will be fired once even if you do reassignments multiple times.

Fixed Issues in 6.9 SP1 Patch 9

Tracking ID	Description
SF-698588 ACM-55408	A null pointer error occurs when the Attribute Synchronization page is accessed.
SF-734427 ACM-57088	The reset password dialogue indicates an incorrect password syntax requirement.
SF-717622 ACM-57090	Custom attributes populate incorrectly in Role > Add Entitlements popup.
SF-669416 ACM-53829	Change request not generated for a review item that is marked with a custom state.
SF-718008 ACM-56669	A report is running on a schedule and the system is emailing the results even though the report "Is Scheduled" setting is NO.
SF-661912 ACM-53199	When a rule remediation is completed and one or more entitlements is revoked, a change request is created to remove the entitlements. Before the change request is completed, a user can cancel it. In such a case, all violating entitlements (associated with the remediation that created the change request), whether they were maintained or revoked, are put in an indeterminate state and the violating entitlements continue to appear as violations of the rule. This situation cannot be resolved for the following reasons: • The violations cannot be remediated because the remediation task was completed, so the violations no longer have an assigned remediator. • The violations are not recognized on any subsequent executions of the rule because when a rule is executed, it only recognizes new violations discovered on that execution of the rule. After applying this patch to the system, when a user cancels a change request that is created by a violation remediation, all of the identified violations are returned to their previous state and a new remediation workflow is created and assigned to the remediator, who can now maintain or revoke the entitlements as required.
SF-728873 ACM-57591	A monitoring policy does not allow the user designated as the monitor to view account change requests for accounts.
SF-736242 ACM-57455	The Remove button turns green after performing a Group Definition Review, when there are no members or entitlements to review. The issue is fixed so that the button displays as red, as it should in this situation.

Tracking ID	Description
SF-691400 ACM-54711	Hebrew characters do not display correctly in workflow approval forms.
SF-685931 ACM-54425	An "ArrayIndexOutOfBoundsException Error - 140" error occurs when a user's Access tab is accessed.
SF-723465 ACM-56394	Cyrillic text is not displayed correctly in reports exported to csv and pdf formats.
SF-669134 ACM-56849	When opening a review from an escalation email, the user would receive an Insufficient Privilege warning.
SF-611399, 651559, 655287, 645137 ACM-51245	An "ArrayIndexOutOfBoundsException Error - 75" error occurs when a user's Access tab is accessed and also in Requests, when selecting to remove access.
SF-645452, 645137 ACM-52790	An "ArrayIndexOutOfBoundsException Error - 74" error occurs when a user's Access tab is accessed and also when selecting a custom attribute in table options..
SF- 640402 ACM-55193	Using the Bulk Action > None option sets already reviewed items to a 'not reviewed' state. The option name was changed to 'Revert to None' to better reflect the action associate with this option.
SF-743615 ACM-57836	Importing reports fails when "CurrentUserID" is included a imported report query.
SF-717191 ACM-56247	An application owner does not have permissions to remove user-account mappings for the application accounts.
SF-17660 ACM-42043	In change requests, if no resource was specified for the fulfillment stage, the request would not be assigned to anyone. This is fixed so that the request will be assigned to the Admin.
SF-683374 ACM-54366	In a request form, unable to set the default value of a radio button based on a user record variable.
SF-741059 ACM-57735	The following workflow error occurs: "ORA-06512: at "AVUSER.ACCESS_REQUEST_PKG", line 314." A request stalls in the Verification Only node of a Work Flow, even though all of the tasks in the job appear to be complete.

Tracking ID	Description
ACM-58159	
SF-659351, 710259, 714047 ACM-53308	Workflow error occurs when evaluating a SQL node that is not in the processing path.
SF-745259 ACM-58128	In an approval workflow, when a request is added, the approvals are being duplicated.
ACM-55959	Form author should be able to set the default selection in a drop-down control.
SF-741340 ACM-57614	Dashboard application tabs inconsistent with other application tabs.
SF-669328 ACM-58070	Access Request form variable (avform.user.Supervisor_Name) is missing.
SF-644170 ACM-54669	Progress bar is not getting updated in account access ownership review.
SF-678067 ACM-54021	Security issue detected in unprotected form variable.
SF-736048 ACM-57094	Deadlock error occurred. Related to this query: "DELETE FROM T_AV_ROLE_MISSINGENTS WHERE ROLE_TYPEID IN (SELECT ROLE_TYPEID FROM GTT_EXP_ROLES)."
SF-741065 ACM-57960	In a request form, the display of answers in a filled form was inconsistent. This was fixed so that variables for fields in a request form display only in the submitted form and not in the Additional Information section.
SF-723895 ACM-56525	Attribute change rules not displayed in the user interface.
SF-748955 ACM-58650	A "java.lang.ArrayIndexOutOfBoundsException" occurs when a user attempts to change his or her password using the external password reset feature.
SF-735998 ACM-57093	An account data collection change verification fails with the following error: "ORA-01652: unable to extend temp segment by 128 in tablespace."
SF-664798	In request forms, the horizontal divider displays incorrectly if the question contains double-quotes. This issue was caused by an encoding error in an HTML control,

Tracking ID	Description
ACM-53630	and has been fixed.
SF-650709 ACM-53946	In an access request, when using multiple approval phases, the most recent comment on an approval was carried forward into the approval email notification. This feature was enhanced so that all comments from the approval appear in the email.
SF-639130 ACM-53947	In an access request, when using multiple approval phases, the comments on an approval are carried forward into the approval email notification, but the comments are not shown in the order they were entered. This has been fixed so that the comments are shown starting with the most recent.
SF-719992 ACM-56295	When creating new accounts as part of an AFX workflow, the email notification that reports workflow variables for user's Full Name and Windows Account ID are not shown in the same order. This is fixed so that the query used to evaluate the changes now guarantees the order, so you can match different variables as needed.
SF-716651 ACM-57228	When trying to edit a workflow, an "invalid number" error occurs and user cannot open workflow. This has been fixed by using the change request ID to identify the workflow, which prevents the error.
SF-589970 ACM-50404	Review escalation that has already fired is firing again after the review definition is edited.
SF-729001 ACM-57087	In a Rules workflow, emails generated using the "Rule Email Reminder" option do not display the Violation Name. This has been fixed so that the Violation Name now displays in the Subject and content of the email.
SF-62225, 638226, 639301 ACM-52283	Change requests are recorded with an incorrect completion date/timestamp. The "Configure TCP/IP and Time Zone Settings on the Appliance" topic in your *6.9 Installation and Upgrade Guide* does not provide instructions on setting the timezone if you are implementing the Oracle Enterprise Manager (OEM). Substitute the "Configure TCP/IP and Time Zone Settings on the Appliance" topic in your *6.9 Installation and Upgrade Guide* with the Configure TCP/IP and Time Zone Settings on the Appliance topic in the Errata section of this document. Step 8 includes updated information.
SF-748108 ACM-58433	Approvals are duplicated after the system was upgraded to 6.9.1 P07 from 6.9.1.
SF-650803 ACM-52857	In attribute synchronization, the change request goes into an error state if the integer type attribute is made null.

Tracking ID	Description
SF-75142, 756354 ACM-58885	Cannot authenticate to AD on port 636 using WebSphere JAAS and RSA IMG authentication.
ACM-52612	Groups are not shown in a user review when assigned to a user's account. For information on the product enhancement related to this issue, see "Review Definitions: Entitlement Filtering" in What's New in 6.9 SP1 Patch 9.
SF-742541 ACM-57844	Change verification from an Active Directory source is failing continuously.
SF-714556 ACM-57205	When more than one workflow email addresses is populated from a workflow variable, only one is used.
SF-745371 ACM-58232	An "ORA-01555: snapshot too old: rollback segment number" error occurs when a large number of users are added to a role. The change request involved stalls.
SF-703754 ACM-57755	LDAP Account Collector: the Group DN is not collected but Accounts are collected successfully.This has been fixed so groups are collected successfully.
SF-754075 ACM-59169	Terminating the user removes an account that has been associated with the user in the past.
SF-728149 ACM-56985	'invalid Type error' appears in the UI when uploading a CSV file to import Entitlement Description for applications.
SF-621894, 683177 ACM-51893	A termination rule creates a change request to disable an account even when Allow Account Disabling is set to NO for an application to which the account provides access. A termination rule now creates a change request to disable an account only when Allow Account Disabling is set to YES for an application to which the account provides access.

Release 6.9.1 Patch 8

Information about the 6.9.1 Patch 8 release is included in the following sections:

What's New in 6.9 SP1 Patch 8

This section lists the features/enhancements introduced in this release.

Feature	What's New
User Access and Account Access and Ownership Review Definitions	On the Content page of the wizard, two options were renamed to better reflect their operation: "Include application roles granted from groups" was changed to "Include direct application roles that are also granted from groups" "Include entitlements granted from groups" was changed to "Include direct entitlements that are also granted from groups"
Review Definition: Account Selection	When selecting accounts to review, you can filter accounts using the Is Disabled and Is Locked attributes.
Review Result: Review Due Date	You can select a new review due date using the date picker in an expired review.
ServiceNow Collectors and Connectors	The collectors and connectors are now compatible with Eureka and FUJI versions of ServiceNow.
Generic SOAP Connector	The connector supports multiple URLs on single connector.

Fixed Issues in 6.9 SP1 Patch 8

Tracking ID	Description
SF-716550 ACM-55976	Cannot edit a role's description from the context of the role when there is an existing description for the role in Admin > Descriptions.
SF-712075 ACM-55722	An indirect entitlement from a technical role a user had from membership in a business role that also included the technical role becomes the user's direct entitlement after the technical role is removed from the business role.

Tracking ID	Description
SF-649574, 707412 ACM-52829	There is an issue with the URL in password reset email notification.
SF-707412 ACM-56559	The "View Password" link in an password reset email notification indicates that a password is unavailable after the recipient enters his or her user name.
SF-22037 ACM-48750	The "Entitlement Raw Name" column cannot be selected from Table Options under the Change Preview tab in Review Results.
SF-596790 ACM-50466	A line break for custom user link text incorrectly occurs on a dashboard.
SF-20111 ACM-46118	AveksaAdmin Login: The system displays the lockout message only after the correct password is entered after the “Maximum number of unsuccessful login attempts" value is exceeded.
SF-628426, 594649, 653522 ACM-52330	On Import of Metadata (XML) with user custom attribute, the attribute value is not displaying on User Review Results. The value of the custom attribute now displays in the appropriate column.
SF-607602 ACM-54667	Rules take three or more hours to execute when using granular filtering.
SF-726390 ACM-56550	Erroneous message "The Oracle version 12.1.0.2 is not supported" displays in the aveksaServer.log during startup and as an initialization warning when viewing system information (Click Admin > System, and select the Diagnostics tab).
SF-713958 ACM-56075	A review dashboard displays twice the number of review assignments.
SF-737142 ACM-57245	Entitlement collection on v6.9.1p4 fails with the following error: "ORA-00001: unique constraint (AVUSER.ECDC_COLLECTION_INDEX_32) violated."
SF-722028 ACM-56257	Identity data unification is taking 2 hours instead of 20 Min after applying v6.9.1 P05.
SF-534283 ACM-50865	The Save button is available to a reviewer who exits a review without making changes to it.
SF-715395	Entitlements are not listed under a user's Access tab and a role's Entitlements tab.

Tracking ID	Description
ACM-56003	
SF-722608 ACM-57053	A user access review still shows subgroup membership that no longer exists.
SF-664137 ACM-55964	When an Active Review workflow was set to change a particular review status (via an Escalation) to Active it did not change the status. The status now changes from OnHold or INActionable states to Active when triggered by the Escalation.
SF-718192 ACM-56121	In user access review, under User Selection tab, an error is displayed on the date format, even though the format is valid.
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-731692 SF-734321 ACM-56847	A "Request could not be handled" error displays when loading the Requests > Configurations > Submission tab.
SF-727917 ACM-56756	Pre-processing of rules appears to hang the system.
SF-682323 ACM-57092	General metadata import failed when the condition was set to resolve all user references using unique attribute:User ID in the export metadata page.
SF-697883 ACM-55367	A change request for a role remains in the pending state even if the role is deleted.
SF-710124 ACM-55896	Problems occurred with a ServiceNow collector connecting to ServiceNow FUJI version. For information, see What's New in 6.9 SP1 Patch 8.
SF-709124 ACM-55622	Command output parameters in an AD AFX connector are not updating the attributes of a pending account.
SF-723738 ACM-54586	In Review Results, when performing a bulk action Maintain or Revoke, when the Sign Off Review Items dialog appears, it shows a Cancel button. This has been fixed to show a Close button.
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

Tracking ID	Description
ACM-56797	review is submitted.
SF-625631 ACM-52094	In group review results, long description and short description options were missing from the table options and information dialogs. These options are now available.
SF-727497 ACM-56600	In Resources > Applications, when viewing an application's detail, the Resource Profile settings include the option to Exclude Entire Application From Add Access And Suggestions. When this option is set to Yes, the application's roles and entitlements should be "not available for request" but instead they were available when comparing two users access. This was fixed so that the option now excludes the roles and entitlements.
SF-730701 ACM-57074	In Requests > Activities, in the By Assignee tab, the Search filter will not properly filter a Role name in the Assignee(s) column. The Search filter now works properly on both users and roles.
SF-715432 ACM-56035	In Roles > Roles, an "insufficient privileges" message appears when attempting to edit a Role when the user editing the Role is defined as either the Business Owner of the Role Set or an 'Other Business Owner' for the Role Set.
SF-727653 ACM-56597	In Users > Groups, in a Group's General tab, if the 'Not available for request' option is set to yes, the group still shows when using the 'compare user' functionality. If one of the users is a member of such a group, it is possible for other users to request and get access to groups that should be inaccessible.
SF-678398 ACM-53980	The due date cannot be updated in an expired review. You can now select a new date using the date picker in an expired review. For more information, see What's New in 6.9 SP1 Patch 8.
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-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-665024 ACM-53364	In a role review, when All sub-components are checked, sub-components on subsequent pages show as unchecked.
SF-604546 ACM-51857	Alternate managers are unable to identify reviewers from outside of a review.
SF-534113	A review only sends out email from email event template, but not from the Reviewer Reassign workflow.

Tracking ID	Description
ACM-49767	
SF-647287 ACM-52856	Cannot complete a fine-grained role definition review when the role has no members.
SF-699090 ACM-55242	A review schedule is invalid if the review is renamed.
SF-589982 ACM-50277	Account attributes (Is Disabled, Is Locked) are not included as filtering attributes in an account review definition. For more information, see What's New in 6.9 SP1 Patch 8.
SF-714534 ACM-56094	Chart element colors revert to the default colors.
SF-698040 ACM-56893	Workflow variables are populated on new workflows, but not on existing workflows.
SF-729969 ACM-56733	Expiration Date attribute is not seen in an account access and ownership review.
SF-730612 ACM-56771	Database caching issue detected for account data that results in a discrepancy between what a multi-app account collector collects and what is observed in the database.
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.

Release 6.9.1 Patch 7

Information about the 6.9.1 Patch 7 release is included in the following sections:

What's New in 6.9 SP1 Patch 7

This section lists the features/enhancements introduced in this release.

Feature	What's New
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	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.

Fixed Issues in 6.9 SP1 Patch 7

Tracking ID	Description
SF-735273 ACM-57068	Change requests in the system indicate they were generated by users who did not generate the requests.
SF-657164 ACM-53336	Adding a node to workflow creates two instances of the node.
SF-725668 ACM-56504	Multiple database deadlock conditions observed.

Tracking ID	Description
SF-705415 ACM-55485	Old change request identifiers are displayed for SoD rule names for violation remediation tasks under Admin > Workflows.
SF-613746 ACM-51548	Unable to create an email template from the context of a review definition.
SF-718060 ACM-56342	The URL link in rule violation remediation email does not display the violations.
SF-706614 ACM-56277	Parallel SQL nodes in a workflow produce inconsistent results.
SF-647498 ACM-52997	The PasswordAvailableExtEvent email event is not triggered for a password reset for an AD authentication source.
SF-727042 ACM-56813	A change request stalls in the approval node after processing over 1000 request items.
SF-725911 ACM-56545	Editing imported local entitlements changes entitlement names to entitlement raw names.
SF-701486 ACM-55171	The Modify button is unavailable for users added to a review by a review refresh.
SF-663079 ACM-53402	In the Bulk Actions window for a multi-step review, the actions options are not aligned with "Explicitly selected."
SF-691107 ACM-17429	Unable to filter on user entitlement attributes in a review definition and in a review.
SF-701868 ACM-55191	A report's display name is the same as the column name.
SF-693570 ACM-54866	Deleted DAG server access still displays in data resource access reviews.
SF-647287 ACM-52856	Cannot complete a fine-grained role definition review when the role has no members.
SF-612345 ACM-51472	A request to grant an entitlement and an account to that entitlement to a user is rejected in the fulfillment phase of a change request. The account, however,

Tracking ID	Description
	appears in the user's Access tab.
SF-671161 ACM-54544	The Entitlements Require Accounts setting for applications are not exported in the metadata.
ACM-54975	The Replace button displayed an incorrect suggested entitlement message in the third phase of a multi-step user a user access review.
SF-721998 ACM-56404	Inability to edit an account collector and to delete a multi-app account collector.
SF-713690 ACM-56589	Data access collection fails with a "ORA-00001: unique constraint" error.
SF-724477 ACM-56433	Performance issues occurred after installing patch v6.9.1p5.
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.
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-685415 ACM-54692	Users not displayed under the Who Has Access tab for an application.
SF-682208, 692154 ACM-55996, ACM-54807	Roles stay in Applied (or Applied New if a new role) state if a change request is partially rejected but still completes successfully
SF-663107, 642394, 654876, 660592, 677237, 677764 ACM-54809	Some role entitlements are incorrectly removed during subsequent collections.

Tracking ID	Description
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-717733 ACM-56045	A null variable in email generated from a workflow displays as ' ' characters.
SF-680826 ACM-54120	Unable to load new jar file into a connector template.
SF-680826 ACM-54112	The MySQL connector does not use the most current version of the jar file: mysql-connector-java-5.1.36-bin.jar
SF-702595 ACM-55250	An Entitlement Rule for a request form question is not able to parse SQL.
SF-711453 ACM-55739	Review performance issues occur after installing 6.8.1.17.
SF-705077 ACM-56002	Completed violating access remediation is indicated as pending.
SF-591397 ACM-52796	A role's members are not cleared as specified by a role membership rule difference rule.
SF-730334 ACM-56776	After a system restart, a change request is processed by the wrong workflow.
SF-731761 ACM-56814	A role's Analytics tab shows missing entitlements not actually missing after entitlement collection is run.
SF-727367 ACM-56574	AFX is not able to auto-provision add/remove group/entitlement for users after 6.9.1 P06 upgrade.
SF-705592 ACM-55365	AD and MainFrame group entitlements disappear from roles after application of P02 or P03 for v6.9.1.
SF-00788341 ACM-63063	While processing a workflow, an exception error pops up due to a large amount of stored node/user data.

Release 6.9.1 Patch 6

Information about the 6.9.1 Patch 6 release is included in the following sections:

What's New in 6.9 SP1 Patch 6

This section lists the features/enhancements introduced in this release.

Feature	What's New
Rules	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.
AFX Connectors	The Salesforce connector supports dynamic variables for its Create Account command. A connector for IBM Security Identity Manager (ISIM) is available.
Workflows	The Provisioning Command node includes a "Wait for Result" option. When it is enabled, the node operates synchronously, waiting for a success or error code callback from AFX before transitioning to the next node in a workflow. The callback captures the status of the command and updates the following job-level static workflow variables that are used in subsequent nodes: • acm.provisioningCommandStatusCode • acm.provisioningCommandStatusMessage Status codes and messages: • 0 - Success • 1 - Failure
Rules: Escalation Workflow	The ability to configure automatic revocation of violating access 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

Feature	What's New
	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.
Change Requests and Workflows	An "Include Terminated Users" option is available for the following access requests components in RSA IMG: • The Add Access and Change Access request buttons when they are configured with the Add Access or Add from request sources action. • A request form User Picker type control. The option is disabled by default. It enables you to request access for terminated users who are scheduled to be reinstated into an enterprise.

Fixed Issues in 6.9 SP1 Patch 6

Tracking ID	Description
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 6.9 SP1 Patch 6.
SF-692095 ACM-55130	Multi-app entitlement collections is taking over 18 hours to complete after installation of v6.8.1 p10.
SF-713690	Unable to delete a data resource set.

Tracking ID	Description
ACM-56105	
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-705986 ACM-55883	The Provisioning - Termination rule does not detect all terminated users.
SF-719308 ACM-56221	Receive an "receive an ORA-00905" error message when saving the queries on a SQL Select node.
SF-639987 ACM-52376	Password challenge questions are not localized for users language choice.
SF-680187 ACM-55131	A deleted role is included under a user's Access tab even though the role has been deleted.
SF-696326 ACM-55082	Log in from an AD authentication source takes an inordinate amount of time.
SF-696638 ACM-54943	A "NullPointerException" error occurs when importing a rule definition that references a non-existent custom attribute.
SF-694923 ACM-54944	Language in advanced search remains in English even when the language is changed in the Options link.
SF-719788 ACM-56120	Infinite looping occurs after editing a role profile.
SF-694001 ACM-55013	Change request with overlapping indirect entitlement items are rejected inconsistently when a role's direct items are partially rejected.
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-689044	Review email is not sent if one of the recipients has an invalid email address.

Tracking ID	Description
ACM-55312	
SF-596925 ACM-51030	The send email action is not executed for an attribute change rule.
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-702306 ACM-55192	The Maintain and Revoke buttons in a review are unresponsive when French is designated as the default language for RSA IMG.
SF-545046 ACM-50059	A request submission question configured to display once is displayed multiple times.
SF-697317 ACM-55069	Role definition reviews are generating change requests to revoke groups from users that are not members of the role.
SF-690180 ACM-54591	A reviewer was unable to undo a sign-off on review items.
SF-647629 ACM-52654	A problem occurs when attempting to create a business description for a set of application roles.
SF-670181 ACM-53938	The AFX Salesforce connector did not support dynamic license variables.
SF-684951 ACM-55148	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 workflow has backup supervisor specified as one of the resources.
SF-698040 ACM-55385	Workflow variable for an application did not return an application raw name.
SF-692241 ACM-55279	A manual change request fulfillment is assigned to AveksaAdmin instead of the asset business owner.
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-623248 ACM-52021	Time out and performance issues occur with change request approvals.

Tracking ID	Description
SF-698100 ACM-55120	Saved report results are missing after an upgrade from v5.1.4 to v6.9.1.
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-679345 ACM-54994	An asset owner is not assigned an approval for a request to provide a group of accounts to a user.
SF-704458 ACM-55311	Duplicates accounts are collected by a multi-app account collector after an upgrade to v6.9.1 P03 from v5.1.4.
SF-700826 ACM-55870	An AFX fulfillment call after an approval did not occur.
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.
ACM-55414	Remediation workflows are not created for all user access rule violations.

Release 6.9.1 Patch 5

Information about the 6.9.1 Patch 5 release is included in the following sections:

What's New in 6.9 SP1 Patch 5

This section lists the features/ enhancements introduced in this release.

Feature	What's New
Rules	Tables that list users with violating access enable you to sort group by and search on custom attributes for those users.

Fixed Issues in 6.9 SP1 Patch 5

Tracking ID	Description
SF-626239 ACM-51949	Clicking on Admin > System > Appliance results in stack trace in the aveksaServer.log file.
SF-695001 ACM-55672, ACM-55344	The Default Identifier field in the User Evaluation window for a role collector did not indicate that User ID is the default identifier for a user.
SF-675297 ACM-53978	Account mappings are removed after a multi-app account data collection even though the "Do not remove accounts when nothing is collected from that application" setting is enabled for the collector.
SF-608691, 625058 ACM-51152	Change verification takes several hours to complete.
SF-628281 ACM-54319	There is no deletion script to delete duplicate violations.
SF-628281 ACM-54865	Existing violations from older version create duplicates when adding an entitlement to a user.
SF-695403 ACM-54935	Role entitlements persist in the application, even though they are not collected.

Tracking ID	Description
SF-695076 ACM-54934	Closed loop remediation verification fails with database caching detected.
ACM-54391	Entitlements directly assigned to accounts are not removed during multi-app entitlement collection.
SF-634173 ACM-52766	V_AVR_USERACCESS view does not give correct values.
ACM-53430	Not all business source owners are assigned a review even though all were specified as reviewers in the review definition.
SF-545924 ACM-49891	A user granted the ability to view approvals in a monitoring policy cannot view the approvals.
SF-689461 ACM-54662	There is an issue with the "Access_Request_Pkg."
SF-668031 ACM-53504	Exceptions assigned to AveksaAdmin using the Review Exceptional Access workflow result in an empty Exceptional Access Grant Details field.
SF-538188 ACM-49730	The Requested On date changes every time the approver clicks the Perform button.
SF-679882 ACM-54277	Active Directory account collector cannot collect from certain domains.
SF-650803 ACM-52857	In attribute synchronization, the change request goes into an error state if the integer type attribute is made null.
SF-681448 ACM-54110	Public database queries failed after an upgrade from 6.8.1 P10 to 6.9.1.
SF-642293 ACM-53369	Request form does not append the values in the non-visual fields when run to create an account.
SF-698118, 681069 ACM-54989	An "Insufficient Privileges" error occurs when attempting to view a user's Request tab.
SF-655400,	Clicking the View Results link in an email results in an "Insufficient Privileges"

Tracking ID	Description
658664,669134, 677434 ACM-52861	error.
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-646251 ACM-52579	The Review Definition: View All entitlement enables users to modify escalation settings.
SF-625568, 620646, 668423, 680413 ACM-52843, ACM-51871	False AFX failures occur when adding or removing user accounts from groups in Active Directory.
SF-682335 ACM-55246	The Collector: Manage and Collector: Admin entitlements are not implemented for the following collectors: • Identity Collector • Unification Config • Account Collector • Role Collector • Entitlement Collector • Multi-App collector • Data Access Collector • App Metadata collector • Scheduling
SF-697835 ACM-54996	Standard SQL regression that works in 6.8.1 patch 9 does not work in 6.8.1 patch 15.
SF-698511 ACM-55189	SSH Connector does not work when there are special characters in data from 6.9.1 P02.

Tracking ID	Description
SF-698511 ACM-55122	Command codes are missing from the SSH connector after upgrading from 6.9 P02 to 6.9.1 P02.
SF-665505 ACM-54430	Items requiring fulfillment are completed by the system when grouped with role changes.
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-21360 ACM-48408	There are duplicate breadcrumbs when drilling down in to requests, approval phase, and supervisor approval.
SF-690230 ACM-54602	The WebService cmd findEntitlements sortDirection parameter is not properly documented.
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-625888 ACM-51925	Membership rule is removed from a role by the role collector when changing, adding, or removing a member that has a missing direct entitlement.
SF-627569 ACM-52088	Action buttons are disabled only for group owner reviewer when using the review results menu.
SF-673360 ACM-54267	Some special characters are not supported for passwords in the Sign-Off field.
SF-626239 ACM-51948	The Admin > System > Settings page shows inconsistent information when the database is remote and the local database has been imported.
SF-665890 ACM-54535	Attribute change rule does not detect the change.
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-694457 ACM-54844	Entitlement collection from an AD source fails due to running out of TEMP tablespace.
SF-705452, 709315	Error occurs during request fulfillment: "ORA-01722: invalid number."

Tracking ID	Description
ACM-55366	
ACM-37817	After remediating a user access rule violation, the following message displays: You have not acted on 1 items. The violation is not remediated completely
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.
ACM-55204	While remediating the violations that are marked with Due Date of a later date, the following message displays: "You have not acted on two items, the violations are not remediated completely."
ACM-53118	Some Aveksa application entitlements are not providing the privileges they are designed to provide.
ACM-53720	The Apply Changes/Revert Changes/Delete privilege disappears when role is combined by Role Owner.
ACM-55519	Collector does not collect future-hire employees from Workday.
ACM-48477	There is no test button for the Provisioning - Joiner/Mover rule.

Release 6.9.1 Patch 4

Information about the 6.9.1 Patch 4 release is included in the following sections:

What's New in 6.9 SP1 Patch 4

This section lists the features/ enhancements introduced in this release.

Feature	What's New
Access Certification	When defining a review, it is possible to filter the entitlements in the review based on attributes of the resource or the resource/action pair, but not attributes of the user entitlement.
AFX - Adapters	All icons are now the same size on the Application Directory Wizard.
Rules	An Activate/Deactivate button is included under the General tab in a rule's details view. You can use it to activate or deactivate a rule, respectively.
Rules	The Closed button has been removed and replaced with a Cleared button and Revoked button. Cleared: In the case of a Segregation of Duty rule, when one of the two sets of entitlements has been revoked, the other set of entitlements is automatically maintained. Revoked: A Revoked entitlement violation is any entitlement that has been revoked and in no longer in Pending Revocation status.
User Interface	The term "review results" replaces "review instances" in review command descriptions in the Web Services Commands table.

Fixed Issues in 6.9 SP1 Patch 4

Tracking ID	Description
SF-543756 ACM-50568	A change request to add members to roles shows incorrect information
SF-637436 ACM-54393	Entitlements are unexpectedly displayed in the customer's view of the Out of Role Entitlement tab.

Tracking ID	Description
SF-539009 ACM-49768	SoD rule with invalid common entitlements lists the same entitlement name instead of each entitlement.
SF-677028 ACM-54005	Edit and Cancel buttons are not enabled when a non-admin user creates a change request using the user ID login.
SF-00681576 ACM-54595	Unification takes longer than expected since upgrading to patch 3.
SF-533888 ACM-52319	Role collector is performing slower than expected.
SF-671320 ACM-54632	A change request is submitted when the Back button is clicked before the Finish button is clicked.
SF-651355 ACM-53366	An attempt to process a Provisioning - Termination rule results in an error.
SF-682323 ACM-54227	General Metadata: Export/Import results in an insufficient privileges error.
SF-672382 ACM-53970	Violation Detection date is newer than the Exception Granted date.
SF-635989 ACM-52306	Exchange 2010 AFX connector documentation in the *RSA IMG AFX Connector Guide* is incorrect.
SF-630667 ACM-53389	In the User Access tab, some users have the same business role assigned multiple times in the review process.
SF-666521 ACM-53975	When a report with AM and PM entries is exported to Excel, all PM values are changes to AM values.
SF-669296 ACM-54106	Alternate Manager Coverage File Upload using Web Services (uploadCoverage) is not working as expected.
SF-665778 ACM-53393	A deleted application's business description is incorrectly retained in the system.
SF-585741 ACM-51589	A decision node in a workflow failed to detect a “contains at least one violation” condition.

Tracking ID	Description
SF-648004 ACM-52968	Workflow is not successfully imported, but the import states it was successful.
SF-692531 ACM-54699	Groups are removed from roles after upgrading to 6.9.1 Patch 2.
SF-684267 ACM-54568	Active Directory group entitlements included in a role are not visible in the user interface.
SF-681527 ACM-54416	Access request form-level approvals call for unapproved items.
SF-622722 ACM-53240	Re-running rules creates new violations instead of adding to existing violations for a user.
SF-607420, 693781 ACM-51072	System administrator has read-only privilege.
SF-671320 ACM-53860	A request form was submitted when the Back button was clicked during a create change request session.
SF-617560 ACM-51670	MySQL Driver doesn't recognize Column Aliasing in Select Statement for Entitlement Collector
SF-694099 ACM-55058	Groups added as entitlements to roles are deleted after the next account collection run.
SF-665505 ACM-54430	Items requiring fulfillment are completed by the system when grouped with role changes.
SF-666487 ACM-53935	Role changes are submitted twice in change requests.
SF-622799 ACM-53163	Java HEAP error occurs regularly after collections for the Model Office environment.
SF-651276, 645804, 639819, 653846, 641001, 666533, 672358, 679297, 677862, 684959 ACM-52718	The Appliance tab on the Admin System page does not load.

Tracking ID	Description
ACM-54350	An entitlement or a member that has been added to a global role and then subsequently removed from the role cannot be added again even though the change request for the add completes successfully.
ACM-53907	Sort and search are not functioning for Custom attributes on the Roles > Roles page.
ACM-54342	Other Business Owner for role set does not associate the role set to the new role.

Release 6.9.1 Patch 3

Information about the 6.9.1 Patch 3 release is included in the following sections:

What's New in 6.9 SP1 Patch 3

This section lists the features/enhancements introduced in this release.

Feature	What's New
AFX Connectors	The SoapWebService connectors supports SSL certificate-based authentication.
AFX Connectors ACM-53412	The Lotus Notes AFX connector supports ID Vault for account creation.
Appliance Updater	The Appliance Updater updates the Red Hat Enterprise Linux 5 operating system.
Data Collectors	Account and Identity data collectors and the "Create AD Directory" wizard include the following changes in SSL configuration options: • The Skip Certificate Validation field is included. • The Certificate field is optional. • The Keystore location field has been removed. How the Skip Certificate Validation and the Certificate options work together: • If the Skip Certificate Validation option is selected and the Certificate field is blank, then an SSL connection is completed without validation. • If the Skip Certificate Validation option is not selected and the Certificate field is blank, then RSA IMG checks the certificate in the default java truststore(cacerts). If that certificate is valid, then an SSL connection is completed. Otherwise, RSA IMG generates an error message. • If the Skip Certificate Validation option is not selected and the Certificate field contains a valid certificate, then an SSL connection

Feature	What's New
	is completed. • If the Skip Certificate Validation option is not selected and the Certificate field contains an invalid certificate, RSA IMG generates an error message.

Fixed Issues in 6.9 SP1 Patch 3

Tracking ID	Description
SF-680823 ACM-54072	The copyright symbol displays as a question mark in the "About" popup.
SF-690006 ACM-54610	The Mark Verified node in a fulfillment workflow is not working after an upgrade from v6.9 P3 to v6.9.1 P2.
SF-670395 ACM-54100	A Supervisor Approval workflow is system-completed regardless of the workflow specification that the business source administrator was assigned the approval.
SF-683601 ACM-54333	A user with the Monitoring:View entitlement is denied access to the Run Details window from Monitoring > Data Runs.
SF-654545 ACM-52874	A ServiceNow account collector stalls after its previous collection run is aborted.
SF-668269 ACM-53476	A user with the Email Admin Role application role or the Email Log : Admin entitlement is denied access to the Email>Log tab.
SF_665053 ACM-53895	A Text Area control type in a request form appears as a Text Field control type.
SF-681801 ACM-54271	A "Request Could not be handled" error occurs when an owner of a rule attempts to edit the rule.
SF-641863 ACM-52396	Attribute change rule notification mail is not displaying correctly.
SF-684282 ACM-54362	An error occurs when attempting to change a RSA Identity Governance and Lifecycle SaaS Admin password.

Tracking ID	Description
SF-675682 ACM-54036	Unable to remediate rule violations after migration from Aveksa Compliance Manager v5 to RSA IMG v6.
SF-539244 ACM-54114	It takes an inordinate amount of time to expand a workflow job grouping.
SF-666385 ACM-53902	Problems with incorrect SQL code in the DATA_RETENTION_PKG..\
SF-602655 ACM-51217	Email template variables are not displayed in Internet Explorer 9 and Internet Explorer 11.
SF-662467 ACM-53201	An identically named group that belongs to two different applications erroneously shares the same business description even though different descriptions were defined for each group in each application.
SF-677224 ACM-54028	The verifyTimeMatch function of /etc/init.d/aveksa_server reports a cryptic failure message when RSA IMG is unable to connect to a remote database as the SYS user.
SF-681718 ACM-54169	/usr/bin/Check_Instance_Running.sh relies on SYS connection instead of AVUSER.
SF-643499 ACM-52659	Inability to localize the review sign-off button.
SF-652060 ACM-52847	An entitlement data collection stalls on the insert into the T_DC_ SOURCEDATA_REJECT_LOG table.
SF-659227 ACM-53094	Editing any authentication source causes other authentication sources configured with a BindDN value containing a backslash character to escape the existing backslashes, which results in authentication failure.
SF-595533 ACM-51479	Invoking a list of approvals from Requests > Approvals takes an inordinate amount of time to load for admin users.
SF-613892 ACM-51477	Invoking a list of approvals from the Approvals icon takes an inordinate amount of time to load for non-admin users.
SF-677616 ACM-53960	A workflow SQL selection node is truncating an SQL statement that worked correctly in a previous version before upgrading to 6.9.1P01.

Tracking ID	Description
SF-616244 ACM-51551	A user with the "Access Request Administrator" security role cannot edit an escalation workflow.
SF-663440 ACM-53599	A "Request could not be handled" error occurs when the Missing Direct Entitlements hyperlink is clicked more than once during an add member to a business role operation.
SF-611868 ACM-53910	The Maintain Revoke actions are still available for members removed from a role in a role review.
SF-19200 ACM-46353	Inability to filter by a user's business unit in an account review.
SF-656453/ 664998 ACM-53473	Several user interface buttons are not working after an upgrade to 6.9 from 5.5.2.
SF-533918 ACM-51614	The "Update_Wf_Emit_Event" call from Access_Request_Pkg is causing database locks and the Login page never appears or is inordinately slow to appear.
SF-20491 ACM-46777	A search by Status = Active does not work in the Rule Definitions window.
SF-642025 ACM-53441	The system ignores the fulfillment/revocation date setting for a change request.
SF-21050 ACM-47395	The migrate.log reports the following error: "ORA-19011 Character string buffer too small."
ACM-48706	Output Parameter to capture an account name did not capture the correct account name after AFX fulfilled a create account request item.
ACM-54273	Issues involving an SSL connection to an Active Directory or LDAP source for identity and account data collectors. See What's New in 6.9 SP1 Patch 3 for more information.

Release 6.9.1 Patch 2

Information about the 6.9.1 Patch 2 release is included in the following sections:

What's New in 6.9 SP1 Patch 2

This section lists the features/enhancements introduced in this release.

Feature	What's New
Access Requests	The following request workflow configuration settings let you enable file attachments in change requests and the actions request approvers and fulfillers can take with attachments: • Show Attachments Tab: Lets you specify whether the tab and its attachments are displayed in a change request. • Add/Delete Attachments: Lets you specify whether approvers and fulfillers can add and delete attachments if the Show Attachments Tab option is enabled. Both options are enabled by default.
AFX Connectors	The following connector types support basic authentication (user name and password) settings: • RESTful Web Service • SOAP Web Service
Password Management/Web Services	Application account passwords can be reset using web services.
Web Services	The following additional account information is returned by the findAccounts web service command: • is disabled • is locked • is orphaned
Web Services	Comments in the return value are now included in the getChangeRequestStatus web service command.
Workflows	The Email tab under Properties for a "Request Completed"

Feature	What's New
	workflow node includes a "User Affected by Change Request" dynamic variable. You can use this variable to specify recipients of change request completed email whose entitlements have been changed by the change request.

Fixed Issues in 6.9 SP1 Patch 2

Tracking ID	Description
SF-661675 ACM-53130	A change request to remove a group from a group remains in the "Pending Verification" state after data collection.
SF-642367 ACM-53026	A role owner is able to revert changes to a role in the "Applied" state.
SF-611297 ACM-51999	A workflow configured to handle all change request items in one job created two approval activities.
SF-586096 ACM-49734	Exported user attribute values are "Yes" for the "In Detail," "In Popup," and "Hide if Empty" settings that have been set to "No" for the attributes.
SF-604024 ACM-51073	Multiple delegations occur when using the "Save and Continue" option in a review.
SF-623432 ACM-51983	Remote agents stopped working after installing 6.8.1.11.
SF-534215 ACM-52987	Rule violation remediators are not updated after remediator reassignment.
SF-600648 ACM-51402	A data access collector fails with this error: "ORA-00001: unique constraint (AVUSER.PK_Y999999_EDC_ENT_DEL_ID) violated."
SF-583278/ ACM-49736	When importing the business description XML using the overwrite option, the rows in the source tables are unstable.
SF-22004 ACM-48648	A database deadlock stalls a user access review.
SF-655400/658664/ 669134	A reviewer is unable to access a review from a link in notification email because of "insufficient privileges."

Tracking ID	Description
ACM-52861	
SF-665890 ACM-53355	A joiner rule is not triggered when an identity that was previously deleted is collected again.
SF-654683 ACM-52932	A change request generated by a role missing entitlements rule incorrectly includes an "enable account" item.
SF-626164 ACM -52077	The date format for the fulfillment phase of a workflow is not consistent with format for the approval phase.
SF-662671 ACM-53243	An attribute change rule with multiple "ALL" conditions is triggered when only one of the conditions is met
SF-638997 ACM-52550	The the database maximum memory heap size setting (Xmx) is overwritten when a patch is installed.
SF-612794 ACM-51571	An "ORA-12899: value too large for column "AVUSER"."T_AV_ WFMILESTONES"."MILESTONE" error occurs when multiple approvers are assigned to a change request.
SF-663339 ACM-53198	Duplicate records observed in a data resource review.
SF-639022 ACM-52305	An error occurred executing a remove a group from an AD server AFX command.
SF-619441 ACM-51678	Inability to upload and manage change request file attachments if Access Request Manager is disabled. For more information, see What's New in 6.9 SP1 Patch 2.
SF-541997 ACM-49321	Incorrect approval assignments are generated for a change request.
SF-21170 ACM-47514	Roles the have been granted indirectly to a user are displayed as directly entitled under the user's access tab, and revoke actions can be executed on them.
SF-642367 ACM-53026	A role owner is able to revert changes to a role in the "Applied" state.
SF-659626	An AirWatch collector fails with a "JSONObject Password not found"

Tracking ID	Description
ACM-53267	error.
SF-539524 ACM-49949	By using a help link, inappropriate access to an appliance’s file system can be gained.
SF-621953 ACM-52029	A change request item to add an account to a group fails with an AFX error.
SF-656277 ACM-52929	When a second change request for a user is rejected, the user's previous change request items are automatically rejected.
SF-666031/ 663017 ACM-51782	Entitlements are incorrectly revoked when a user's role is revoked in a user access review.
SF-628647 ACM-52400	AFX _PKG commits after each insert statement. This results in excessive CPU usage.

Release 6.9.1 Patch 1

Information about the 6.9.1 Patch 1 release is included in the following sections:

What's New in 6.9 SP1 Patch 1

This section lists the features/enhancements introduced in this release.

Feature	What's New
Access Request Button Action	An "Add/Remove using request sources" action for a request button is available. It specifies that both the Add and Remove actions are available on an entitlement selection table, the Add action for entitlements a user does not have and the Remove action for entitlements a user has. This action is applicable only if the request form used to process the request allows both add and remove actions in an entitlement selection table.
Account Access and Ownership Reviews	The following options enable a review designer to prevent reviewers and monitors, respectively, from taking any action on their accounts (shared accounts included): • The "Allow reviewers to review their own accounts" configuration option is available under the review definition's Reviewers tab. • The "Allow monitors to monitor their own accounts" configuration option is available under the review definition's Monitors tab.
Appliance Database	The "Run Backup Now" button has been removed from the Admin > System > Backup window. You can still schedule backups from the window.
Appliance Updater	The appliance updater detects if the installation is a soft appliance environment In this case, it only applies Oracle database patches.
Attributes	An integer attribute can accommodate a Long.MaxValue, 2^63 value. In earlier product versions, it was 2^31.
Aveksa Application Data Collectors	The capability to create new collectors for the application and to edit and inactive the data collectors included with the application has been removed.

Feature	What's New
Change Requests and Workflows	By default, a fulfillment activity does not display comments entered for change request items by request approvers. To display the comments, you can enter the following runtime variable under the Form Properties tab for the Manual Fulfillment node: ${jobUserDataChangeRequestItemx2ExComment}
Database Export/Import dmp File Options	Ability to define the path of a file created by avdbexport and read by avdbimport and specify that the file is compressed. The syntax examples demonstrate both options. Export Syntax Example: ./AVDB_Export_AVUSER.sh -o <dir> -g Where: -o <dir> = Directory for the output file -g = Flag indicating the file should be gzipped Import Syntax Example: ./AVDB_Import_AVUSER.sh -i <dir> -g Where: -i <dir> = Directory for the input file -g = Flag indicating the file is gzipped
Language Options	This release includes updates for the following language options: • Chinese (China) • Chinese (Taiwan) • French • German • Italian • Japanese • Portuguese (Brazil) • Russian • Spanish (Mexico)
Review Coverage File	The "Account" subject type is supported. Define a reviewer example:

Feature	What's New
	userid='sAdams'|account|1=1|ent|1=1|review Define a monitor example: userid='fClark'|account|1=1|ent|1=1|read_write|
Workflows: SOAP and REST Web Service Nodes	Retry logic has been provided for SOAP and REST Web Service workflow nodes. Whenever the node makes a HTTP/HTTPS connection to an external server and the connection fails (network/time out issues), it will automatically attempt to connect again.
Workflows: SOAP Web Service Node	The SOAP Web Service node supports SSL connection to an endpoint. The node properties window includes a "WS-Security" tab. The tab provides the following SSL configuration options: • The "Enable WS-Security" option • Input fields for private key, keystore, and X.509 certificate settings

Fixed Issues

Tracking ID	Description
SF-656832 ACM-52938	A user is not granted the local entitlements in a role when the user is added to the role.
SF-640866 ACM-52418	An Exchange connector creates an incorrect email address.
SF-16653 ACM-40345	An "Oracle, ORA-06564: object AVEKSA_DATA_DIRECTORY does not exist, errors during import" error occurred during a database import.
SF-642581 ACM-52478	A concurrency error occurs when reassigning an approval.
SF-634698 ACM-52740	Local entitlements are not showing up under a user's Access table after a change request is completed.
SF-00622384 ACM-51897	When the customized Change button is clicked in a review definition, there is no indication based on the color of the button that the change was previously reviewed.
SF-610186	When the Back button in a form is selected by a user, the default value for the

Tracking ID	Description
ACM-51196	user is not updated.
SF-16442 ACM-40668	Exceptional access is displayed for entitlements revoked as a result of a segregation of duties rule violation.
SF-539251 ACM-49105	Performance issues occurred with reviews.
SF-617854 ACM-52517	A password change request cannot be created.
SF-00615361 ACM-51641	When the first activity in a change request is completed, the Mark Verified node auto-completes other activities.
SF-21707 ACM-48161	The Search function on the change access page does not work correctly for the following values: • <greater than> • <greater than or equal to > Vs <less than> • <less than or equal to>
SF-640870 ACM-52532	A request button URL can be manipulated to override the user restriction filter.
SF-645238 ACM-52756	Coverage files do not support account mappings in data resource access reviews. For more information, see What's New in 6.9 SP1 Patch 1.
SF-663283 ACM-53196	SoD rule violation counts are not displayed in a user access review.
SF-642163 ACM-52562	Incorrect group membership for roles when the same group name exists in more than one application.
SF-616934 ACM-51769	A role owner loses role privileges when the owner changes the owner but does not apply changes
SF-627007 ACM-52217	The number of members in a role review is not identical to the number of members in the role after the role is altered.
SF-647878 ACM-52791	A roaming user subfolder is not created by the Create Account command using the AFX Lotus Notes connector.

Tracking ID	Description
SF-636204 ACM-52360	An entitlement data collection fails with this error: "ORA-00001: unique constraint (AVUSER.ECDC_COLLECTION_INDEX_42) violated."
SF-616391 ACM-52723	An Active Directory account data collector has unmapped several accounts.
SF-646552 ACM-52648	The SOAP Envelope dialog box for a SOAP connector is truncating values that are inserted into it.
SF-655465 ACM-52875	The "Specifying System Settings" section in the *Administrators Guide* does not cite or describe the purpose of the AveksaAdmin Email setting. AveksaAdmin requires an email address for AveksaAdmin password resets.
SF-585326 ACM-52158	The "UserAccountControl" attribute value is not collected.
SF-18022 ACM-42697	Patch installation script does not check for free space before installing the EAR.
SF-633619 ACM-52264	A Lotus Notes collector does not collect all resources.
SF-646777 ACM-52608	Users with "System Administrator" or"Access Requests Administrator" Aveksa application roles cannot work with Password Management features.
SF-612924 ACM-51503	A cluster initialization error occurs on WebSphere.
SF-595923 ACM-51427	An account is created for a user entitlement request despite the fact that the request was canceled in the approval phase.
SF-610175 ACM-52465	A change request fulfiller is only provided information regarding a revoke and not an add when the custom "Modify" review option is completed.
SF-612453/ 641109 ACM-37812	The password re-use restriction is not enforced.
SF-21945 ACM-48654	An "patch.sh: line 256: jar: command not found" occurred after installing a v6.8.1 patch.

Tracking ID	Description
SF-596444 ACM-52351	A review monitor is able to reassign review items even though the review definition specifies that monitors are not allowed to reassign.
SF-653369 ACM-52767	Role Missing Entitlements rule fails when it is processed.
SF-20294 ACM-46634	No change request was generated when a user was added to a role during a role definition review.
SF-617854 ACM-52170	Unable to log in to RSA IMG using ADC authentication.
SF-16927 ACM-45233	Active Directory sub domains are not collected.
SF-596869/ 636057/639796 ACM-50596	An error occurs when a Reassign node is passed a legitimate value.
SF-580431 ACM-50231	A change request fulfillment activity does not include comments entered by reviewers for review items. For more information on the solution, see What's New in 6.9 SP1 Patch 1.
ACM-53158	The add member action in a role review does not generate a change request.
SF-582755 ACM-49820	A provisioning joiner/mover rule is not suggesting business roles when it is configured to suggest roles.
ACM-52652	SOAP and REST Webservices nodes - Parser fails when the response contains namespaces.
ACM-52072	Data resource flag not cleared for groups after entitlement data collection.
ACM-51997	An appliance was detected doing frequent outbound request to an external IP address. The IP address is related to ehcache (cache used by AFX MMC Console) that tries to access Terracotta.org to check for updates.
ACM-52373	The "java.lang.RuntimeException: Illegal TXN State" exception occurs after applying 6.9.0 Patch 3.

Release 6.9 Service Pack 1

The RSA IMG Release 6.9 Service Pack 1 *Release Notes* include the following sections:

RSA IMG 6.9 Service Pack 1 Documentation

Documentation released with the RSA IMG 6.9 Service Pack 1 includes:

- *Release Notes* (this document), with a Documentation Supplement
- *RSA IMG Upgrade Guide 6.9 Service Pack 1*

Use the RSA IMG 6.9 documentation set with the RSA IMG 6.9 Service Pack 1 release. The *Release Notes* includes documentation for the new features in the Documentation Supplement section, and updates to the exiting documentation topics in the Documentation Errata section.

Upgrading to RSA IMG 6.9 Service Pack 1

The *RSA IMG Upgrade Guide* provides instructions for upgrading RSA IMG software in the following scenarios:

- RSA appliance running RSA IMG V 5.x or later.
- Non-RSA appliance or server running RSA IMG V 5.x or later.
- Application server (WebLogic or WebSphere) running RSA IMG V 5.x or later.

If your installation is not covered by one of these scenarios, the following table lists other possible upgrade scenarios and the appropriate action that you must take to perform the upgrade:

Scenario	Action
System running RSA IMG 4.x	Back up your existing system and perform a new installation as described in the *RSA IMG Installation Guide V6.9*.
Access Fulfillment Express (AFX)	If you are currently running AFX version 2.0.x or 2.5.x, upgrade RSA IMG as described in this *Upgrade Guide* and then upgrade AFX as described in chapter 2 of the *Access Fulfillment Express Guide V2.9*. If you are currently running AFX v 2.8.1 (also known as V6.8.1) or V6.9, AFX is upgraded automatically after upgrading to RSA

Scenario	Action
	IMG V6.9 Service Pack 1 and restarting RSA IMG. These *Release Notes* contain a number of updated topics related to AFX. Before upgrading AFX, see the updated AFX information in the Documentation Errata section.

What's New in Release 6.9 Service Pack 1

This section lists the features/enhancements introduced in this release.

Documentation

The existing 6.9 documentation was not updated for this release. However, these *Release Notes* list new features in this section, and include a Documentation Supplement that addresses new features in more detail. The only new documentation included for this release is the *RSA IMG V6.9 Service Pack 1 Upgrade Guide*, which is designed to ease migration from previous versions. If you are upgrading an existing version of RSA IMG, download the new *Upgrade Guide* from the SCOL site.

Feature	What's New
Access Requests: Notification Email to Subsequent Approver	RSA IMG notifies approvers via email that the action for a change request has been completed when a change request approval workflow specifies multiple approvers and one of those approvers rejects a change request. The system does not generate notification email for approvers who are logged into the system and attempt to take action on an approval after another approver has rejected the change request. In this case, the system displays a message to those approvers that the change request approval has been completed.
Access Requests: User's Request Tab	A user's Requests tab consolidates all completed and pending request records in single table. You can use the following Show options to filter the requests you want to view: • All • Pending • Completed Grouping options are also available. You can, for example, group requests by requester, request date, and other request attributes.
Appliance Database	The "Run Backup Now" button has been removed from the Admin > System > Backup window. To back up the database, see

Feature	What's New
	"Schedule Database Backups" in chapter 2 of the *RSA IMG Administrators Guide V6.9*.
Attributes: Accounts	When configuring attributes, you can add up to 20 custom account attributes of type "string." Previous releases of RSA IMG were limited to 10 custom account attributes of type "string."
Attributes: Display in Table	When configuring a custom attribute, you can choose to display or hide the attribute in table views by selecting or deselecting In Tables.
Compatible Remote Oracle Database Versions	RSA IMG supports the following Oracle versions in remote database installation scenarios: • Oracle 11.2.0.3 • Oracle 11.2.0.4 • Oracle 12.1.0.1
Connectors and Collectors	RSA IMG V6.9 Service Pack 1 includes connectors and collectors for the following applications: • Google DFP • ISIM 6.x • Java (generic) • EPIC (using the provided RESTful Connector. **Note:** Contact Customer Support for a document explaining how to use the RESTful connector and web services with EPIC.)
Collectors: Creating from Outside of a Business Source	You can create account collectors and entitlement collectors from outside the context of a directory or application. The summary screens for account collectors and entitlement collectors include a Create Collector button that allows users with system administrator privileges to create these types of collectors from within the summary screen.
Exceptional Access Table Enhancements	The Rule Name, Rule Type, and Rule Description columns are available in Exceptional Access tables.
Modify Host Name Script: Server Certificate Creation	The modifyhostname.sh script creates new RSA IMG server certificates when it runs to modify the appliance hostname. If AFX is implemented in your installation, you must update its

Feature	What's New
	client certificates to include the new hostname. For more information, see Change an AFX Server SSL Certificate.
Password Management: Allow Users One-Time Identity Confirmation Using Their Attribute Values	The Identity Confirmation module allows you to specify the identity attributes a user can provide to validate his or her identity during a user password reset session. Users are required to enter their user name or account name or both to reset their passwords. You can also specify that users enter additional attributes to confirm their identity. Identity attribute validation applies only to users who have not registered their password reset challenge questions. Users are restricted to one password reset attempt using identity attribute validation. The "Require Users to Enroll their Challenge Questions" password management setting lets you specify that users validating their identity with attributes must enroll their challenge questions before they can complete their reset. For more information, see Identity Confirmation Method for Password Resets in the Documentation Supplement.
Password Management: Attribute Synchronization Usage Safeguards	RSA IMG generates warning messages in the user interface to alert an administrator user about the ramifications for application or directory participation in attribute synchronization when the administrator attempts the following actions: • Attempts to change the password policy for an application/directory that is participating in password synchronization. • An administrator attempts to delete the password policy for an application/directory that is participating in password synchronization. If an administrator persists with the change or delete action, the applications/directories are deleted from the password synchronization group. The Business Source link in the Configure General Properties settings window for a new user form replaces the previous Directory link. It allows you to select any directory that meets the aforementioned requirements.
Password Management:	The password management "External Password Reset information

Feature	What's New
Customizable Password Reset Prompt Text	Configuration" settings allows you to customize the text that appears in the sequence of windows in which a user enters identity validation information during a password reset session.
Password Management: Request Workflows Configuration	All request workflows provided by RSA IMG are configured by default to auto-approve requests for user password resets and password synchronization. The workflows include the following nodes that evaluate whether a request is for a user password reset or a password synchronization: • Reset Password • Synchronize Password
Password Management: Challenge Question Email Settings	You can configure the system to send email notifications to users to enroll their challenge questions. For more information, see Password Management Settings in the Documentation Supplement.
Provisioning: Support for Additional Directories	You can onboard a new user into any data repository directory that meets the following requirements: • The directory is associated with an active account data collector. • The directory is associated with an active identity collector. • The directory must have an AFX connector mapped to it that is configured to create an account. The Business Source link in the Configure General Properties settings window for a new user form replaces the previous Directory link, and allows you to select any directory that meets the requirements listed above.
Public Database Schema	The Account table includes an ORPHAN_DATE column.
Remote Database Configuration: Time Zone Verification	A procedure for verifying the timezone settings within a remote database is included in the *Database Setup and Management Guide*. For more information, see Verify Correct Database Configuration.
Reporting: Template for Audit Events	The pre-defined report template Audit Events for the Past 30 Days allows you to create a tabular Audit report that lists the most recent audit events, for example, administrator logins or changes to system settings.

Feature	What's New
Request Forms: Enhanced Entitlement Table Control	The "Select only one entitlement" configuration option lets you specify that a requestor is limited to selecting a single entitlement from the entitlement table. This option is disabled if the "Subject Must/May Have One Entitlement" option is selected for the "Change Item Handling" setting.
Reviews: Account Access and Ownership	You can define a new Account Access and Ownership review that displays the accounts to be reviewed only, with none of the entitlements associated with the accounts. The reviewer is restricted to either maintaining or revoking an account rather than having the ability to manage account entitlements. To define such a review, when creating a new review definition for an Account Access and Ownership Review, clear all the items in the Contents screen under Select the types of items to be reviewed.
Reviews: Entitlement Replacement Option	The "State" tab page for a user access review definition includes a "Replace" option. It lets you configure the review so that reviewers can replace an existing entitlement in a review with another entitlement of the same type for the same business source. This action generates a change request that includes a remove item (for the replaced entitlement) and an add item (for the replacement entitlement). You can restrict this option to particular users under review and by entitlement type. For granular entitlements, you can restrict replacement entitlements to those with actions to the same resource.
Reviews: Escalations	The Mark Review Items node in the Mark as Revoked review escalation includes a setting that lets you specify whether the revoked review items are indicated as revoked by the reviewer or the system.
Reviews: Monitor Options	When creating or modifying a User Access review, you can specify the following as monitors of the review: • **Supervisors of the users being reviewed.** Specifies that supervisors of the users are granted monitoring privileges. Previously, this option specified that the supervisors of the supervisors of the users being reviewed were granted the monitoring privileges. • **Supervisors of the reviewers.** Specifies that supervisors of the reviewers are granted monitoring privileges. This allows supervisors to monitor the review items of their subordinates who are

Feature	What's New
	performing reviews. If you choose role owners as reviewers, this option specifies that supervisors of the role owners are granted monitoring privileges.
Reviews: Reassigning Review Items	When reassigning items during a review, the reviewer can add comments to explain the reasons for reassigning the item. To include these comments in the email that is sent to the newly assigned reviewer as a result of the reassignment, you must configure the email template reviewItemReassignEvent to include the variable "reviewItemDelegatedComments."
Reviews: Show Instructions Option	When creating or editing review definitions, you can specify whether or not the Review Instructions display by default in reviews. Check or clear the Show Instructions box in the General screen or General tab.
Role Collectors	When creating a role collector for Active Directory and Database data source types, you can map a Backup Owner just as you can map the Owner. The Role Backup Owner attribute is the name of the attribute from a role entry that stores the unique role backup owner name/ID. If this property is not set, then the collector does not extract a role backup owner.
Roles Account Template	You can specify a default "roles account template" in the "Account Template" section under the Requests tab for a business source. A roles account template specifies the parameters for the accounts that must be manually created for a user who is added to a role. Regardless of what other account templates are associated with a business source, the default roles account template is included in a change request in the following scenarios: • A new member is added to a role that has entitlements from a single application that is associated with multiple account templates. • A new member is added to a the role that has entitlements from multiple applications that are associated with multiple account templates.
RSA Archer GRC Integration	RSA IMG provides easy integration with RSA Archer GRC using the RSA IMG application wizard. For more information,

Feature	What's New
	download the RSA Archer Application Access Governance Solution Guide, available from RSA SecureCare Online at http://knowledge.rsasecurity.com.
Rules: Bulk Violation Assignment	When reassigning rule violations, you can assign multiple violations at the same time, and assign those violations to more than one remediator. For more information, see Reassign Rule Remediation Tasks in Bulk in the Documentation Supplement.
Rules: Dynamic Violation Assignment	You can dynamically assign rule violation remediators based on an identity attribute of the user in violation under the Resources tab for the following rule workflow nodes: • Rule Remediation • Secondary Rule Remediation In previous versions of RSA IMG, you could not dynamically assign a remediator based on a violating user attribute.
Rules: Exceptional Access Review	RSA IMG allows you to configure a two-phase remediation process when an assigned remediator chooses to maintain exceptional access for a user with violating access. You can specify a second remediator to review the business justification for the exceptional access granted by the first remediator. The second remediator can then chose to maintain or revoke the exceptional access grant. RSA IMG provides the "Review Exceptional Access" rule workflow as an example of how to use two-phase remediation. This rule workflow applies to remediation of user access and segregation of duties rule types. For more information, see Configure a Two-Step Remediation Rule Action in the Documentation Supplement.
Rules: Violation Remediation	Reassignment History: The Rule Violation details window includes a History tab that lists all remediation task reassignments for the violation. The tab also allows administrators to enter and view comments about the reassignments. Violation Reassignment: Rule administrators can reassign open rule violations by accessing the rule violation details window.
System Settings: Environment Naming	You can configure a name for an RSA IMG deployment. The Systems Settings tab contains an Environment section that allows

Feature	What's New
	you to specify a name for the RSA IMG system in the Name field. The name is displayed in the user interface, workflows, statistics reports, and exported XML data.
Upgrade: Improvement	During an upgrade, RSA IMG V6.9 Service Pack 1 intelligently migrates the database by running only the necessary processes required to update to the new version. As only the necessary components are updated, customers may now experience a faster migration and less downtime during an upgrade.
User Interface: Ability to Upload a Custom Favicon	You can override the default favicon icon that is displayed by the aveksa.ico file in Firefox, Internet Explorer, and Chrome browsers by uploading a favicon.ico icon file. You upload the file in the User Interface > Files window. You must reload the user interface to display the custom icon after the upload.
User Interface: Manage the Display of the Logout Confirmation Prompt	The Show confirmation when logging out setting under Admin > User Interface lets you specify whether users are required to confirm whether they want to log out from an RSA IMG session.
User Interface: Settings	The following user interface configuration setting groups, previously located under Admin > System > Settings are located under Admin > User Interface > Settings: • User Session • Menus • Table Defaults • Info Popup Dialog Contents • Other Features Users with the "User Interface : Admin" entitlement for the Aveksa application can access and edit the user interface settings The Custom Help URL setting lets you specify an alternative source of help to the help source provided by RSA IMG. This URL is invoked from all help links throughout the user interface.
User Registration: Ability to Create Naming Transforms	You can create and manage JavaScript base name transforms for naming policies. The naming policies you create can include up to 10 input parameters, and you can edit and delete all user-created transforms. Note: You cannot edit or delete the four base name transforms provided by RSA IMG.

Feature	What's New
	For more information, see Create a Base Name Transform in the Documentation Supplement.
Web Services	When using web services you can enable a user to make requests on behalf of another user. In such a case, the user making the request is known as a request delegate. For more information, see Delegating Requests Using Web Services in the Documentation Supplement.
Workflows: Monitoring Jobs	When viewing workflow jobs, you can filter which jobs display by the following job states: • All • Active • Completed • Error state
Workflows: REST and SOAP WebService Nodes	Two new workflow nodes that support web services interaction with other applications that provide web services capabilities are now available for inclusion in approval and fulfillment workflows: • The REST WebService node invokes a REST call to an endpoint. • The SOAP WebService node invokes a SOAP call to an endpoint. The responses and results from the calls are stored in the workflow variables based on the configuration in the node.This information can be used in a work flow's decision logic. The "Proceed on failure" error handling option in the Resources tab for the nodes lets you specify whether you want the workflow that includes the node to proceed or stall if the call to an endpoint fails. For more information, see: • Configure a REST Web Service Node • Configure a SOAP Web Service Node

Fixed Issues

Tracking ID	Description
SF-19190 ACM-44873	Table column sorting does not work in the Monitoring window's Schedule Information table.
SF-21644 ACM-48302	No ability to limit entitlement tables to a single selection in a request form.
SF-637358 ACM-52256	A user's Expiring Password table displays not only the user's expiring passwords but those for all other users.
SF-21050 ACM-47395	The migrate.log reports the following error: "ORA-19011 Character string buffer too small."
SF-19283 ACM-45676	When provided a variable that contains a quote delimiter, it is possible to create an error within the workflow by passing a single quote and then a colon. When creating a SQL query that contains a quote delimiter containing a single quote and then a colon, the colon is removed when the query is saved.
SF-19682, 20726 ACM-36819	Active Directory requests fail when the account or group contains a comma.
SF-20899 ACM-47427	If user results are grouped and ordered, the user interface sometimes displays duplicates for results that require a page change to view entire list.
SF-19825, 21205, 589057 ACM-45964	The Aveksa application can be renamed, which causes errors.
SF-20157 ACM-46256	The user name is not displayed in emails that use the account template.
SF-19142 ACM-47791	Each time the Collection process is run, the Business Entitlement Description processing takes increasingly longer to execute.
SF-22141 ACM-48778	When the Table Column options are set to default, the Reject button is disabled.
ACM-48779	Rejected buttons are disabled when "All Changes" on the approval page are moved or when a new column is added using the table options.

Tracking ID	Description
SF-21811 ACM-48497	The “Enter” button does not execute a password submission in a review.
SF-21214 ACM-47667	Role metadata changes are not reverted.
SF- 539533 ACM-49092	Requester is able to approve the request without appropriate permission by just changing the OID in a request URL.
SF-22207 ACM-48823, 48786	Approver action and comments are not retained.
SF- 544573, 582267 ACM-49611	Line breaks are not rendered in review emails when "No markup allowed" or "Allow sanitized HTML" security settings are specified.
ACM-49553	Inability to specify Saleforce connector proxy settings.
SF- 580501 ACM-49628	An “add member to a role” action is fulfilled by AFX even after the “revert” action (to not add member) is performed on the role.
SF-20858 ACM-48864	Attribute change rule failed to detect an attribute change.
SF-21843 ACM-48378	Workflow SQL parser does not recognize quote delimiters when using form variables.
SF- 545686 ACM-50064	Query from “V_COMMON_SOD_RULE_ENTS” takes an inordinate amount of time to complete.
ACM-51474	The "Maintain" and "Revoke" buttons can be selected concurrently in a user access review.
SF-543545 ACM-49316	The web services “List of IPs allowed to invoke web services” setting reverts back to the default setting after the IMG server is restarted.
SF-19484 ACM-46114	User Entitlement is missing from the User Access tab if a user entitlement change request is performed at the same time the user account is created.
SF-539121 ACM-49289,	Users with View All entitlements can complete the following tasks: • cancel a request

Tracking ID	Description
49290, 49291, 49292, 49293, 49294, 49295, 49296, 49297, 49104	• change outbound events • cancel all pending runs • create a business holiday calendar • create an email template • delete all inactive runs • delete dashboard components • edit a connection • edit email template
SF-21638, 604267 ACM-48583	Suggested entitlement is not shown in the Default Provisioning Form.
SF-595792 ACM-46966	ADC does not perform as expected.
SF-593446, 593451 ACM-50717, 50716	Cross site scripting is observed.
SF-534145 ACM-49104	Users with View All Role permissions are allowed to edit an email template from a Review Definition.
SF-602816 ACM-50748	Users with Business Owner and Business Unit Business Owner roles cannot see business roles.
SF-616971 ACM-51525	When creating a new role, the Existing Role Set menu is not sorted.
SF-611399 ACM-51245	Error-75 occurred on user access tab and while entitlements were being revoked.
SF-22102 ACM-48930	Date field in a request form displays "undefined" when a date is entered.
SF-623618 ACM-52018	Account collector deletion action stalls.

Tracking ID	Description
SF-534209 ACM-49241	While editing an entitlement data collector, window 3 takes an inordinate amount of time to load.
SF-627941 ACM-52049, 49303	Inability to collect account and group GUID values.
SF-605516 ACM-51044	Provisioning-joiner/mover rule is triggered after collection instead of after identity data unification.
SF-22309, 21284 ACM-48963, 47686	An advanced supervisor filter in a request form is not saved.
SF-596265 ACM-50506	The sqljdbc.jar driver file is excluded from the WAS RSA IMG distribution because it is incompatible with WAS 6.1. The sqljdbc.jar file is now included the distribution.
ACM-52037	CN validation error occurs when AFX executes a create account command on an LDAP server.
SF-615720 ACM-51447	The Provisioning - Joiner/Mover rule is producing unexpected results.
SF-600108 ACM-50665	The Role Membership Rule Difference is still processing this role and creating CRs
SF-20601 ACM-49725	Explicit creation of new certificates is required after running the modifyhostname.sh script. For more information on how this issue was addressed, see What's New in Release 6.9 Service Pack 1 and Configure TCP/IP and Time Zone Settings on the Appliance.
SF-614278 ACM-51470	Overly high SQL submits to the t_av_files table over the course of an hour.
SF-18413, 591128 ACM-43509	Attribute separator is not included in a metadata export.
SF-625607 ACM-51984	Delimiter is fixed in a request form field with a web service control type.

Tracking ID	Description
SF-21050 ACM-47395	The migrate.log reports an "ORA-19011 Character string buffer too small" error after migration from v5.5.8.
SF-618117 ACM-51563	Search criteria entered for User Changes in one change request displays changes from all change requests.
SF-17131 ACM-41221	The Changes to Approve view of User Changes in change request cannot be filtered correctly.
SF-20209, 534006 ACM-46464	Response from RESTful web service: Cannot bind to address - No component registered on that endpoint.
SF-19953, 19955, 20797 ACM-45961	The RESTful web service connector encodes the slash character ("/") in a connection URL to this set of characters: "%2F."
SF-533883, 534205 ACM-51156	Entitlement data collection fails with this error: "unique constraint (AVUSER.ECDC_COLLECTION_INDEX_32) violated."
SF-15636, 18969, 19792 ACM-38854	Oracle SYS account expires on an appliance. For more information, see Create a Database User Password Profile.
SF-20947 ACM-47446	AFX is unable to update Active Directory (AD) for a user who has multiple accounts in the AD directory.
SF-16693 ACM-40729	Installation error occurs on a virtual machine.
SF-596443 ACM-50746	The following installation error occurs: "PRVG-9023 : Manual fix up command "/tmp/CVU_12.1.0.1.0_oracle/runfixup.sh" was not issued by root."
SF-201316 ACM-46557	Unable to log in to an appliance in ANSI mode.
SF-21159 ACM-48613	Approval comment text rendered incorrectly.
SF-538192 ACM-49030	User changes not displayed in a change request details view.

Tracking ID	Description
SF-14934, 17875 ACM-37418	The afxinstall script fails if you do not provide a fully qualified installation directory path.
SF-616383 ACM-46123	No documentation available on how to install/upgrade a database driver user for collections.
SF-20776 ACM-47718	Inconsistent functionality of the Edit Allowed After Submission workflow configuration setting.
SF-21302 ACM-47781	Review generation takes an inordinate amount of time to complete.
SF-534353, 590698 ACM-48950	The User Id column is not available in a role's Members table.
SF-20413 ACM-46758	Review items automatically revoked by the Mark as Revoked escalation workflow indicate that the assigned reviewer revoked the items instead of the system.
SF-20138, 20826 ACM-46346	No constraint on the t_system_settings.parameter that will prevent the entry of an identical parameter value.
SF-20606 ACM-47066	Cross-frame scripting protection lacking.
SF-16653 ACM-40345	Database restoration results in an "Oracle, ORA-06564: object AVEKSA_DATA_DIRECTORY does not exist" errors
SF-20254 ACM-46914	Running a statistics report results in errors if a table exists in the schema with mixed case.
SF-20721, 533953 ACM-47132	A role export does not include description data when the same role is imported into another system.
SF-21097 ACM-47462	Attribute value not exported and imported.
SF-600696 ACM-51418	The CASCADE=>TRUE is not included on our database calls to DBMS_STATS to insure that INDEXes are included
SF-20419	An ORPHAN_DATE column is not included in the T_AV_ACCOUNTS

Tracking ID	Description
ACM-46895	public schema objects.
SF-20923, 534034 ACM-47524	The Remove (Some) option does not work in a entitlement table.
ACM-42526	Account does not show on group entitlements within a segregation of duties rule remediation task.
SF-534046, 21276 ACM-48734	The value of the Public level variable is not returned by the SQL Select node into the calling workflow.
SF-21945 ACM-48860	Nonsensical "[lf][lf]" characters appear in the description for a workflow.
ACM-49176	Criteria for a product entitlement is not viewable.
SF-602683 ACM-50778	SiteMinder collection fails with a "java.lang.UnsatisfiedLinkError" error.
SF-533968, 22330, 533935, 20163 ACM-49226	Identity collection results in a duplicate user error.
SF-20910 ACM-50914	Paging error messages in the log for a Novell identity data collector.
SF-553352, 600033 ACM-47725	A "String out of range -1" error occurs while attempting to set a public variable for an SQL Select workflow node.
SF-19834, 539704 ACM-46428, 49963	When choosing an option from a drop-down menu on the home dashboard, the URL briefly flashes on the screen (Internet Explorer only).
SF-18329 ACM-44031	Any user without a first name selected by a filter in a user access review definition is not retained in the filter.
SF-595733 ACM-50549	Various operational issues observed using RSA IMG on Internet Explorer v9.
SF-18814 ACM-44285	Form fields are displaying question mark ("?") characters.

Tracking ID	Description
SF-10645 ACM-26085	Sun IdM fulfillment handler fails.
SF-18142 ACM-43437	The *AFX Guide* does not provide adequate information about the "Upload Missing Files" indicator for connector templates.
SF-20410 ACM-46836	The *Installation and Upgrade on WebSphere Guide* and the *Installation and Upgrade on WebLogic Guide* do not provide adequate information about SSO HTTP header authentication.
SF-21252 ACM-48281	The *User Tasks Guide* did not indicate that the "Users review their own entitlements" option is valid only if the "Allow reviewers to review their own user entitlements option" under "Additional Settings" is also selected in a user access review definition.
SF-20845 ACM-47111	The “Please fill in default values” pop up message appears in a report preview after default values have been provided.
SF-589505 ACM-50013	The Submission configuration window does not adequately indicate that its settings apply to explicit requests submitted from a user's Access tab or from a request form.
SF-21939 ACM-48744	Inability to configure the time server setting on an appliance with a SUSE Linux operating system.
SF-583579 ACM-50155	Unable to edit activity node escalations when the Access Request Manager module is disabled
SF-20372 ACM-47209	When using an account table on a request form and the accounts have a custom attribute, the value of the custom attribute is not displayed.
SF-20004 ACM-46463	Tables in forms are not correctly updating the value passed to them from a radio button object type if they have already been passed a value.
SF-586941 ACM-49811	There are unnecessary check boxes in the table in the Manage Access window.
SF-21995 ACM-48737	The business source value is not displayed in a change request to add a group entitlement.
SF-21301 ACM-47681	Extraneous characters are displayed in forms that contain static text of an image type.

Tracking ID	Description
ACM-39283	Exceptional access continues past expiration date.
ACM-27140	Defects observed in a statistics report.
SF-21791 ACM-48316	A selected tab is not maintained when working in a review.
ACM-46518	Hyphens and underscores are not valid characters in form field variable names.
SF-20849 ACM-47782	Change verification after account collection taking an inordinate amount of time to complete.
SF-21507 ACM-48156	The Attachment tab is included in an approval despite the fact that Access Request Manager is disabled.
SF-18421 ACM-44674	The Exceptional Access view is not displaying maintained entitlements in violation of a segregation of duties rule.
SF-631063 ACM-52395	A hibernate error occurs on the Rule Violations window.

Documentation Supplement

The following sections contain additions to the RSA IMG documentation. The RSA IMG documentation set was not updated for the 6.9 Service Pack 1.

Accessing RSA IMG Request Forms from an External Portal

RSA IMG allows users to access and launch Access Request forms from an external website or program within their organization.

Prerequisites

- Create or select an Access Request form within the RSA IMG Platform that will be called from the external website or program.
- The web application developer must have a solid grasp of web services and how to use them in the external website application.

  Note: While both username & password pair and Web SSO methods are supported for obtaining a valid user session token using web services, RSA recommends that you use the Web Service SSO authentication for better user experience.

Procedure

1. On the RSA IMG menu, click Admin > Web Services and review the existing RSA IMG Web Services that you will use in the external web application to launch the Access Request form.
   You must use the external web services command, externalform, to configure a link between the website or program and the Access Request form.
   The externalform web service command must include the following parameters:
   - token- Use the loginUser web service command to obtain a valid user token to validate that the user is authorized to access and launch the access request form.
     The loginUser token is passed with the externalform web service command using:
     token=<Value>
   - formName - Use the findForms web service command to find the name of the access request form you want to access.
     The findForms result is passed with the externalForm web service command using:
     formName=<Value>
   - prevURL - Use the prevURL web service command to identify the page where the user will be redirected when the user completes or cancels the external access request form.

The Base64-encoded URL value is passed into the externalform web service command using: **prevURL=<Value>**

Note: This command is specific to the implementation of the external web application and the value must be Base64-encoded. If this parameter is not passed with the externalform web service command and the user cancels out of the Access Request form, the message "Access to form is aborted" is displayed in a new browser window. The message is available in string.properties and can be modified based on requirements.

- Oid (optional) - If necessary, use findApplications web services command to retrieve the application Object ID to associate a specific application with the Access Request form.

  The findApplications result is passed with the externalform web service command using: **Oid=<Value>**

2. Add the listed parameters to the externalform web service call within the external web application.

   External request form URL example:

   ```
   http://<ip>:<port>/aveksa/externalform?formName=<Value>&Oid=<Value>&token=<Value>&prevURL=<Value>
   ```

Configuring Access to a Data Source

You must specify how collectors access data from various data sources from information provided to you from data source administrators. This involves specifying the source (host name, file name, or URL for example) and the particular credentials or parameters (user name and password, BindDN, or driver class for example) required by the collector to gain access to and extract the data.

For example:

- If you are configuring a collector to extract data from an Active Directory or other LDAP implementation, RSA IMG displays a connection window where you configure parameters that let the collector connect to the LDAP server.

  Settings include the LDAP host name, the LDAP port (389 is the default), and the authentication credentials: the Bind DN and Bind Password. You can also specify whether to use an SSL connection for LDAP data transfer.

  Note: By default, ordinary LDAP searches are received through port 389/636(ssl) and Global Catalog (GC) searches through port 3268/3269(ssl). So, when you use any base dn (User base dn for example) from the root domain/forest(“DC=DEMO,DC=Local” for example) you should use port 3268/3269(ssl) so that the search occurs on GC. If the server attempted over port 3268 is not a GC server, the server refuses the bind. Use the default port if it’s not a GC server.

- If you are configuring a collector to extract data from a flat file (for example, a CVS or fixed position type) RSA IMG displays a configuration window that lets you specify the user and group file names, user and group row patterns, user and group row and column separator characters, and user and group unique name column headings.
- For an LDIF (Lightweight Directory Interchange Format) file data source, RSA IMG displays a configuration window that lets you specify in an identity collector where to locate users in the LDIF file:
  - LDIF File Path: The path of the LDIF file.
  - objectClass: The object class filter to retrieve users.
  - Base DN: The base DN to retrieve users.
  - User Id: The value of the attribute specified in this field for the User Id.

  See LDIF Configuration Information for an Account Collector and LDIF Configuration Information for an Entitlement Collector for more information.

Note: For flat file data source configurations you can select the XML option if you would rather enter configuration information in XML format.

After you finish configuring a collector, you should test the validity of the access/connection settings. See Testing Collectors for more information.

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 IMG, 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 IMG users table. Any attribute of a unified user can be configured to perform this comparison. The user is then authenticated and an RSA IMG 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 IMG 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 IMG login screen is displayed to the user.
- LogoffURL (optional) — Enter the URL for which a user is redirected to when logging off from RSA IMG. 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 IMG; 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 IMG 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 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 IMG 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 IMG, 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.

Configure Processing Schedules and Triggers

You can automate rule processing by configuring scheduling and process triggering settings for rules.

Procedure

1. Click Rules > Configuration.
2. Click Edit.
3. To create a global schedule for one or more rule types, under Rules Processing, do the following:
   a. For Scheduled, click Yes.
   b. Select when the schedule begins. Click Now to begin immediately, or click Date, and choose the date to begin from the calendar.
   c. For Frequency, select how often (daily, weekly, monthly and so on) you want the rules to be processed.
   d. For Rule Type, check the rules that you want to process according to the schedule.

   Note: To remove a rule type from the schedule, deselect the rule. To remove the schedule for all rule types, click No for the Scheduled option.
4. Specify the actions (any type of data collection or identity unification as applicable) upon which RSA IMG processes rules. Under Rule Processing Triggers, select the processing option for one or more rule types.

   Note: To remove automatic processing triggers for one or more rules types, deselect the rule types. RSA IMG does not process the deselected rule types.
5. Under Exceptional Access, specify the default and the maximum number of days that a user who is in violation of a rule is granted exceptional access.
6. Under Options, specify whether or not rule designers can override global scheduling and rule trigger settings.

- To allow rule designers to override settings, select Allow execution of segregation of duties rules with common entitlements.
- To remove the ability to override settings, clear Allow execution of segregation of duties rules with common entitlements.

7. Under Options, specify whether or not you want to allow common entitlements in a segregation of duties (SoD) rule. To allow common entitlements, check Allow execution of segregation of duties rules with common entitlements.

   Note: Normally, when the system processes an SoD rule that has common entitlements, it flags the rule as invalid. When this option is selected, processing the rule does not change the status of the rule. However, deselecting this setting may result in the system flagging SoD rules with common entitlements as invalid when an administrator modifies the rule and the system processes the rule.

8. Click OK. The scheduling and process trigger specifications take effect immediately.

Password Management Settings

This section lists and describes settings you configure to manage how you want password resets processed for RSA IMG users.

Field	Description
Password Synchronization	Enables the Password Synchronization module.
Identity Confirmation	Enables the Identity Confirmation module. For more information, see Identity Confirmation Method for Password Resets.
Send enrollment emails to users	Enables system-generated reminder email to users who have not yet enrolled their password challenge questions. This enables administrators to designate an opportune time for RSA IMG to generate the email, which can consume a substantial amount of system CPU resources.
Challenge Questions Email Batch Size	Specifies the maximum number of challenge question enrollment reminder emails generated at a time by RSA IMG.
Challenge Questions Email Frequency	Specifies the frequency with which RSA IMG generates batch challenge question enrollment reminder emails.
Notify users when Challenge Questions are changed/updated	Specifies whether RSA IMG generates the notification email.

Field	Description
External Password Reset URL	Specifies the RSA IMG host URL where the external password reset form is located. A password reset requester uses to the form to validate his or her identity. Local host is an example value only. You must overwrite this value with the correct URL.
External Password Reset Logo	Specifies whether the external password reset form includes the default logo or a custom logo.
Require Users to Enroll their Challenge Questions	Specifies whether users who have yet to enroll their questions are required to when they attempt a password reset by providing one or more attribute values to confirm their identity. This is applicable only when the Identity Confirmation module is enabled and configured to prompt users to provide identity attribute values for confirmation. For more information, see Identity Confirmation Method for Password Resets.
External Password Reset information Configuration	Enables you to customize .the text on an external password reset form.

Identity Confirmation Method for Password Resets

Use the password management Identity Confirmation module to provide a method to validate users that have not enrolled their challenge questions for an external password reset. This is an optional module.

You configure identity confirmation as follows:

- You must specify that a user provides one or both of their primary attributes, user name and account name to validate their identity.
- You can specify additional attributes that a user must provided to validate his or her identity.
- Users are restricted to one reset attempt using identity confirmation.

You can require that these users must enroll their questions during the reset process by enabling the "Require Users to Enroll their Challenge Questions" password management setting.

Configure Identity Confirmation Settings

Procedure

1. From the Requests menu, click Password Management.
2. Click Identity Confirmation.
3. Click Edit.

4. Select one or both primary user attributes,and specify whether users must enter either (OR) or both (AND) to validate their identity.
5. Specify additional attributes users must provide. Specify attributes the user is sure to know, First Name and Last Name for example.
6. Specify any additional identity confirmation attributes users must provide.
7. Click OK.

Delegating Requests Using Web Services

When using web services you can enable a user to make requests on behalf of another user. These requests are known as delegated requests and the user making the request is known as a request delegate.

You can configure an individual user as the request delegate for another user, and you can configure an individual user as the request delegate for all users. In the latter case, the user may log in using a service account that is used specifically for making requests on behalf of other users.

The web services request command createChangeRequest includes the tag <OnBehalfOf>, which specifies the name of the user for whom the request is being made. For example, if user jbrown wants to make a request for user kgray, the tag is <OnBehalfOf>kgray</OnBehalfOf>. If the user that is logged in to the web service is not authorized to act on behalf of a user, and attempts to make a request for the user, an error is generated and logged.

Enable a User to Make Requests on Behalf of Another User from a Web Service

Assigning a user as a request delegate enables the delegate to make requests on behalf of a user.

Procedure

1. Click Users > Users.
2. Click the user name of the user upon whose behalf requests will be made.
3. Click Edit Attributes.
4. In the Request Delegates field, click Edit.
5. Select the user name of the delegate and click OK.
6. Click OK.

Enable a User to Make Requests on Behalf of All Users

Enabling a user to make requests for all users allows you to configure a single account as the one source of delegated requests. Typically, when granting a user this ability, the intent is to funnel all requests through a single account, for example, if you want to configure the account as a portal for all delegated requests.

Procedure

1. Click Requests > Requests.
2. Click Create Request and select Add Access.
3. Click Aveksa.
4. Check the name of the request delegate, and click Next.
5. Add the entitlement User:Delegate Web Service Requestor and click Next.

   (Optional) Enter a Description, Notes, a Fulfillment Date and a Revocation Date.
6. Click Finish.

View Users Who Can Make Requests on Behalf of Another User from a Web Service

If you have assigned request delegates to a user, you can view the delegates in the user record.

Procedure

1. Click Users > Users.
2. Click the name of the user.
3. In the Request Delegates field, view the names of any users who can make requests on behalf of this user.

Configure a REST Web Service Node

Before You Begin

- You must have a working knowledge of the REST architectural style to configure the node.
- Decide how you want to use the node: the information you want the node to get and how you want the information consumed in the workflow.

Procedure

1. Select the node.
2. In Properties, configure the following settings:

Setting	What You Enter
General	Description (optional)
Request	Endpoint URL and one of the following verb types: • GET: Request parameters names and values • POST: Full request body
Proxy	Proxy settings that enable connection to the endpoint
Header	Header parameters
Authentication	Authentication credentials that enable connection to the endpoint
Response	Configuration components: • Response configuration to parse and save the data from the REST response to workflow variables • The Proceed on failure setting that specifies whether the workflow proceeds if the REST call fails • Error variables that save information about a call failure that stalls a workflow

3. Save your configuration settings.

See Also
Workflow Node Descriptions

Configure a SOAP Web Service Node

Before You Begin

- You must have a working knowledge of the SOAP XML-based messaging protocol to configure the node.
- Decide how you want to use the node: the information you want the node to get and how you want the information consumed in the workflow.

Procedure

1. Select the node
2. In Properties, configure the following settings:

Setting	What You Enter
General	Description (optional)
Request	Configuration components: • Endpoint URL • SOAP request envelope.
Proxy	Proxy settings that enable connection to the endpoint
Header	Configuration components: • SOAP action • Header parameters
Authentication	Authentication credentials that enable connection to the endpoint
WS-Security	The SOAP Web Service node supports SSL connection to an endpoint. Configuration options: • The "Enable WS-Security" option • Input fields for private key, keystore, and X.509 certificate settings
Response	Configuration components: • Response configuration to parse and save the data from the SOAP response to workflow variables • The Proceed on failure setting that specifies whether the workflow proceeds if the SOAP call fails • Error variables that save information about a call failure that stalls a workflow

3. Save your configuration settings.

See Also
Workflow Node Descriptions

Reassign Rule Violation Remediation Tasks

Users whose privileges include Rule: Admin can reassign rule violation remediation tasks to one or more users.

Procedure

1. Reassign violation remediation assignments. Select the remediation tasks using one of the following methods:
   - Select by violation. Click Rules > Violations.
   - Select by user access or segregation of duties rule:
     a. Click Rules > Definitions.
     b. Select the rule for which you want to view violation remediation assignments.
     c. Click the Violation Remediation tab.
2. Check the remediation tasks you want to reassign.
3. Click Reassign.
4. Select one or more users to which you want to reassign the tasks.
5. Enter comments.
6. Click OK.

Configure a Two-Step Remediation Rule Action

This section applies to user access and segregation of duties rule definitions only. The following procedure uses the actual Review Exceptional Access workflow, but RSA IMG provides this workflow as an example upon which you can base your own two-step remediation process.

Procedure

1. In the rule definition, select the Violation Remediation action and then select the Review Exceptional Access workflow.
2. Specify remediators in the rule definition as required.

   Note: You can also specify remediators in the Review Exceptional Access workflow as described next in this procedure.
3. From the Rules menu, select Workflows.
4. Click the Review Exceptional Access workflow.

5. Click Edit Workflow.
6. Specify remediators as required under Resources in the Rule Remediation node properties.
7. Specify one or more secondary remediators under Resources in the Secondary Rule Remediation node properties. The default remediator is AveksaAdmin.

Change an AFX Server SSL Certificate

You must change the AFX server's SSL certificate when the certificate has been changed in RSA IMG. For example, if you updated the server.keystore certificate to SHA-256 you must update an AFX server's client certificate to SHA-256.

Procedure

1. Click the AFX menu and select Servers.
2. Select the server for which you want to update the SSL certificate.
3. Click Change Certificate.
4. Click OK in the Change Certificate window.
5. Click Download Keystore and save the client.keystore file on your computer.
6. Copy the client.keystore file to <AFX-home>/esb/conf
7. Restart AFX.

Create a Base Name Transform

You can create as many different JavaScript base name transforms as you require for your naming policies. Your transforms can include up to 10 input parameters entered in a register user request form.

Note: You must have at least a basic proficiency with JavaScript to create base name transforms.

Procedure

1. From the Requests menu, select Configuration.
2. Select Naming Policies.
3. Under the Base Name Transforms table, click New.
4. Enter a Name and Description.

5. Accept or change the default firstName and lastName default parameters. Add other identity parameters as required. You may, for example, want a transform to render a name from a user's first name, last name, and job code values entered in a request form.
6. Edit the default JavaScript code in the Definition box, or enter new code to produce the transform result you require for a naming policy.
7. (Optional) Enter the output you expect in the Sample Result box. You can compare the expected result to the actual result when you test the transform.
8. Test the transform. Enter examples of the text you want rendered by the transform, and then click Test.
9. Revise the transform as required if the test does not produce the result you expected.
10. Click OK.

The transform you created is added to the Base Name Transforms table and can be included in any of your naming policies.

Managing System Security

RSA IMG security settings enable you to specify the following security requisites:

- The level of protection you want to provide against brute-force login attempts into the system, password reset attempts, and the login lockout duration when a login attempt or password reset attempt threshold is reached.
- The level of protection you want to provide the system against cross-site scripting attacks launched from input provided into text fields in the user interface.

  Cross-site scripting security options:

  - No markup input is allowed in any text field in the user interface — Data in this state passes though a sanitizer that removes any HTML markup and scripting. (The markup is filtered out, not encoded.) This is the system's default configuration.
  - Sanitized HTML input is allowed in text fields — Data in this state passes through a sanitizer that removes any HTML markup not on a specific whitelist (see for more information). The whitelist includes nothing that allows scripting.
  - Allow any markup in particular text fields — Data is not filtered or encoded. Any HTML markup or scripting can be entered in text fields.

- Whether secure login sessions (HTTPS) are required for client login sessions.
- RSA Identity Governance and Lifecycle Mobile web services session timeout parameters.

It also lets you upload a server.keystore file when you are required to upload the file, such as for migrating certificates from SHA-1 to SHA-256 after an upgrade.

Procedure

1. Click the Admin menu and select System.
2. Click the Security tab.
   The Security Settings window appears.
3. Click Edit.
4. Configure settings listed and described in the following table:

Option	Description
Security	Lets you specify the following session login and password reset attempt settings: Maximum number of unsuccessful login attempts: Lets you specify the number of failed login attempts a user is allowed. The default value is three failed attempts. The user is denied any further opportunity to log in after the last failed maximum attempt for the duration specified by the “Lockout period” setting. You can also specify that unlimited attempts are allowed. See for more information. Maximum number of unsuccessful password reset attempts: Lets you specify the number of failed password reset attempts a user is allowed. A user entering an invalid user name or failing to answer password reset challenge questions results in a reset failure. The default value is three failed attempts. The user is denied any further opportunity to reset a password after the last failed maximum attempt for the duration specified by the “Lockout period” setting. You can also specify that unlimited attempts are allowed. Lockout period: Lets you specify the number of minutes after a user fails the maximum number of attempts to login or reset a password before either can be attempted again. The default value is 15 minutes. You can also specify that no lockout period ensues for maximum failed attempts. Whenever a user is locked out upon failing to login or to reset a password the maximum number of times allowed, the system generates

Option	Description
	a “User Lockout” admin error. See for information on viewing admin errors and configuring system-generated email notification of admin errors for system administrators. Enable secure session cookie: Lets you specify whether secure (HTTPS) connection only (Yes) is allowed from browsers. The system prevents users from logging into RSA IMG from unsecure connections if this option is enabled. See for more information on password security features. Server Certificate Store for Agent SSL Connections: Lets you download the server.keystore file. Master Encryption Key Storage Directory: The directory where the master key is stored. The default directory for hardware and software appliances is: /home/oracle/security Key Rollover/Data Re-encryption: Lets you generate new (roll over) Data Encryption Keys (DEKs), which are used to encrypt data in RSA IMG . Additionally, you can choose to roll over the Key Encryption Key (KEK), which is used to encrypt the data encryption keys. After performing a key rollover, the system uses the new keys to encrypt any new data that must be encrypted. Data encrypted with a previous key remains encrypted with that key until the data is re-encrypted or given new values. For more information, see Roll Over Encryption Keys/Re-encrypt Data.
XSS/Scripting Security	Allow HTML/Javascript in these input fields: All of the following settings are set to No markup allowed by default to prevent cross-site scripting attacks. Select Allow sanitized HTML or Allow any markup were applicable only as required. • All fields in RSA IMG - The system renders sanitized HTML in the user interface. • Descriptions - The system does or does not render sanitized HTML entered for business description fields: raw name, long description, tooltip text. • Email Body (Templates, Review Emails) - The system does or does not render sanitized HTML entered in the body of email generated by the system. • Request Form Questions and Static Text - The system does or does not

Option	Description
	render sanitized HTML entered in static text fields in forms or it accepts any markup. • Login Page Message - The system does or does not render sanitized HTML entered for custom login instructions or it accepts any markup. • Request Instructions - The system does or does not render sanitized HTML entered for request instructions or it accepts any markup. • Review Instructions - The system does or does not render sanitized HTML entered for review instructions or it accepts any markup. Allow UI to be embedded in another application's frame: Prevents the RSA IMG user interface from being embedded in another application's frame for security reasons (cross-frame scripting attacks are possible in some browsers). The default value is No. **Note:** RSA IMG displays warnings about the security ramifications of allowing any markup in input fields.
Web Services and Mobile	Lets you specify settings for RSA Identity Governance and Lifecycle Mobile sessions. Require secure connections: Lets you specify whether secure connections are required for the following web services commands: • GetSecuritySettings • KeepAlive • LoginUser • LogoutUser • FindApprovals • GetApprovalDetails • GetApprovalsForUser • GetRequestItems • PerformApproval The default setting is Yes, which means that these web services commands must be issued via a secure (HTTPS) connection. Session inactivity timeout: Lets you specify the amount of time a mobile session is inactive before it expires. For example, a user has exited a

Option	Description
	session but has not logged out. The default is 10 minutes. Session lifetime timeout: Lets you specify the amount of time a session exists before it expires. The default is 120 minutes. Allow mobile app to save username setting: Lets you specify whether the mobile session prompts users to save their login user names. The default setting is No. See for more information. See for more information on web services commands.

See Also
Roll Over Encryption Keys/Re-encrypt Data
Allowed Markup Input Whitelist

Specifying Review State Options

A review state defines an action a reviewer can take on a review item in a review. The Maintain and Revoke state options are available for all review types. You can configure other state options for particular review types. For more information, see Review Definition State Options.

You can customize review state options as follows:

- Provide a custom display name for a state. For example, you may want to replace "Revoke" with "Remove" or some other term.

  Note: Custom names are displayed “as is” if they are not translated in the customerstrings.properties file or in a localized version (customerstrings_de.properties or customerstrings_fr.properties for example.) Consult your RSA IMG administrator for assistance as required.

- Specify that reviewers must provide comments to complete an action. Comments provide other reviewers, review monitors, and auditors with information about why an action was taken on a review item.
- Specify a default review state of None or Maintain for all items in a review.Reviewers must take action on all review items in the None state, and reviewers can override the Maintain state for review items they do not want maintained.

- Specify that reviewers can provide an expiration date for review items they maintain. This is useful for reviews of temporary employees who only require an entitlement for a particular interval.
- Specify that a review item revocation is nullified if the resulting change request is rejected.

For information on configuring review states for a review definition, see Configure Review State Options.

Review Definition State Options

State	Description
Maintain	Default state option for all review types. Maintains an entitlement indefinitely or temporarily for a specific duration if the "Allow expiration" option is selected. You would typically allow reviewers to specify an entitlement expiration date for a temporary employee.
Revoke	Default state option for all review types. Revokes an entitlement.
Replace	Optional review state for user access reviews only. Replaces an entitlement in a review with another. This action generates a change request with an item to remove the current entitlement and an item to add the replacement entitlement. For this state, you can specify the users to which it applies and the type of entitlement that can be replaced. Reviewers are restricted to replacing entitlements with those from the same business source. For example, a user under review has an entitlement to a Finance application. The reviewer chooses the Replace action for the entitlement. The review displays a list of entitlements only for the Finance application from which the reviewer can choose a replacement entitlement. For granular entitlements, however, you can specify that any granular entitlements for any resource type are available as replacements by selecting the Allow resource changes for fine grained entitlements option. Otherwise, reviewers can only replace granular entitlements with those for the same resource.
Disable	Optional review state for account access and ownership reviews only. Disables an account for a business source that supports account disabling.You can use this option in conjunction with the Lock and Unlock options.
Enable	Optional review state for account access and ownership reviews only. Enables an account for a business source that supports account enabling. You can use

State	Description
	this option in conjunction with the Lock and Unlock options.
Lock	Optional review state for account access and ownership reviews only. Locks an account for a business source that supports account locking. You can use this option in conjunction with the Enable and Disable options.
Unlock	Optional review state for account access and ownership reviews only. Unlocks an account for a business source that supports account unlocking. You can use this option in conjunction with the Enable and Disable options.
Custom	Select the This is a valid review state option if you want to create an optional review item state name that reviewers can apply to a review item. For example, you may want to define a state name that connotes that a review item is under consideration, not revoked or maintained, but in an indeterminate state pending final resolution. You can also specify that a Custom state is essentially identical to the Revoke state by selecting the Generates change request option.
Additional Settings	Lets you specify the following settings: • Default state displayed for review items: ◦ None — Requires reviewers to explicitly choose whether to maintain, revoke, or perform any other available action on their review items. ◦ Maintain — Requires reviewers to explicitly choose whether to revoke their review items or perform any other available action on their review items. You can choose this option to streamline the process for reviewers so they do not have to explicitly maintain review items in review types where few items are typically revoked. If you have customized the Maintain state display name, that name appears in the review. **Note:** The default state setting is not available for role, data resource access, and data resource ownership reviews. • Revert revoked items if change request is rejected — Specifies that revoked review items are reverted back to the default state if change requests generated from the review are rejected.

Configure Review State Options

Procedure

1. While creating or editing a review definition, click the States tab.
2. Select the states you want to provide in the review and customize review state options as required. For more information, see Review Definition State Options.
3. Click OK.

Replace an Entitlement in a User Access Review

You may have the option to replace a user's entitlement to a particular business source with another to the same source in your review. Consult your review administrator if you have questions about the scope of entitlements you can select as replacements.

Procedure

1. Open the user access review assigned to you.
2. Click the Replace button for an entitlement you want to replace.
3. Select the replacement entitlement and enter a comment justifying your action. You may be required to enter a comment to proceed with the entitlement selection.
4. Click OK.

   A change request generated from the review includes two change request items: one to add the replacement entitlement and one to remove the replaced entitlement.

Documentation Errata

This section includes corrections to the v6.9 RSA IMG document set.

Get RSA Software Installation Packages

Note: The following text replaces the section "Get RSA Software Installation Packages" in the *RSA IMG Installation Guide V6.9*. The names of many of the installation files have been revised to 6.9.1 from 6.9.

All installation and upgrade files are accessible from RSA Link at https://community.rsa.com/community/products/governance-and-lifecycle. To download the necessary files, you must have a valid license for RSA IMG.

Download the following installation packages:

- wildfly-8.2.0.Final.tar
- openjdk17_v001.tar.bz2
- aveksa-<product version>.tar.bz2

Download these files for a local database implementation when upgrading to Oracle 12.1.0.2:

Note: Upgrading to Oracle 12.1.0.2 is required when upgrading to RSA IMG 7.0.

- linuxamd64_12102_database_1of2.zip
- linuxamd64_12102_database_2of2.zip
- linuxamd64_12102_grid_1of2.zip
- linuxamd64_12102_grid_2of2.zip
- oracle_12.1.0.2_patches_v001.zip
- asmlib-008_x64.tar.bz2
- cvupack_Linux_x86_64.zip
- redhat-release-6Server-1.noarch.rpm (Download this file if you have a non-RSA appliance or server running Red Hat Linux 6)

Download these files for an off-the-appliance database implementation:

- instantclient-basiclite-linux.x64-12.1.0.2.0.zip
- instantclient-sqlplus-linux.x64-12.1.0.2.0.zip

You must copy these files to a DVD and then copy them to your appliance as described in Copy Installation/Upgrade File Packages to Your Appliance or Server in the *Installation Guide*.

Get the Operating System Installation Software and Create the Installation DVD

You must download operating system installation files to a computer (not the appliance) from RSA Link at https://community.rsa.com/community/products/governance-and-lifecycle and create the installation DVD that you will use to install the operating system on the appliance.

Procedure

1. Log in to RSA Link and download the image:

   `dvd-SLES-11SP3-ACM-7.0.0.iso`

2. Burn the iso file image (do not copy as a data file) to the DVD using any industry-standard DVD burner product. See the DVD burner documentation for details.

System Requirements for a Server

Note: This content replaces "System Requirements for a Server" in Chapter 5: "Software Installation Setup" in the *Installation and Upgrade Guide*. It includes updated information about the requirement that disk space must be partitioned in the root directory and that Oracle must have a static IP address for RSA IMG installations on a VMware virtual machine.

RSA requires that the compatible customer-provided installation server meets all hardware and software requirements for RSA IMG v6.9 installation. New servers requires SUSE Enterprise Linux 11 SP 3 64-bit. Existing servers on RHEL 5u3 and 5u8 are supported for upgrades to existing installations.

Recommended Hardware/System Configurations

This section describes hardware/system requirements for the following environments.

- **Deployment.** Intended for doing the deployment work, staging and functional testing for example, not for use in large multi-user deployments.
- **Production.** Designed for typical enterprise deployments up to 500 concurrent users, up to 1000 applications, and up to 20 million entitlements.

Component	Requirement (Development Environment)	Requirement (Production Environment)
RAM	16 GB - 32 GB	32 GB - 256 GB

Component	Requirement (Development Environment)	Requirement (Production Environment)
Processor	Intel E5-2400 Quad Core	Dual Intel E5-2400 Quad Core
Hard Disk	450 GB (RAID 1 or RAID 5)	1 TB + (RAID 1 or RAID 5)

Recommended Disk Partitioning Guidelines

Swap size: minimum swap size should be configured relative to system memory size.

Memory < 2 GB	Min. Swap = 3 GB
Memory 2GB -16GB	Min Swap = Memory Size
Memory >16GB	Min Swap = 16 GB

RSA IMG can be installed with a local database (on the appliance) or can connect to a customer-provided database on a remote host system. The installation process assumes that the root partition is configured according to recommendations. The installation process will create any required directories from that partition as needed, /home/oracle for example.

Operating system partition (root): 16GB minimum, 100GB recommended (database not included). 325GB minimum, 1.1TB recommended (non ASM installation)

An installation with a local database using ASM requires a separate database partition: 300GB minimum, 1TB recommended.

Required Software on the Server

The following 64-bit operating system must be installed:

- SUSE Enterprise Linux 11 SP3 64-bit
- RedHat RHEL 5u10 and up, 64-bit; RHEL 6u5 and up, 64-bit. Ensure that required Oracle 12.1.0.2 prerequisite packages for RedHat are installed. You may refer to Oracle's documentation for more information.

Server Configuration Prerequisites

- Make sure that there is at least 8GB of free space in the /tmp directory.
- For remote database installation instances, ensure that the TCP port 1555 or the TCP port that you have provided is available to be reached.

  Note: To check whether or not your TCP port is reachable, you can run the following command:

  `telnet db-hostname.example.com <TCP port>`

  Where `<TCP port>` is the TCP port you have provided.

Once you've confirmed that your TCP port has connected successfully, press the control key and the “]” key together to get back to the command prompt. If your TCP port does not connect successfully, contact your IT Database team about your connectivity issues.

- Installation of the Oracle database has additional requirements:
  - Only one root user , a user with (UID=0), can exist
  - Root user must have a umask of 0022
  - Oracle has sufficient disk space and permissions. Oracle will install in the directory /u01
  - There is an entry in the /etc/hosts file that does not resolve to 127.0.0.1
  - A Network Time Protocol (NTP) server is configured and responding
- JBoss server requires the following ports to be available for use:
  - 8443: JBoss application server https port
  - 8444: ACM http port for agents, web services, and the workflow compiler
  - 8080: ACM https port for agents and web services

About Installation on a VMware Virtual Machine

Note: The Oracle database installed with RSA IMG platform requires a static IP address. DHCP is not supported.

Installing RSA IMG on a VMware virtual machine is no different than installing it on a physical machine. The VMware administrator simply creates a virtual machine that matches the hardware and software requirements mentioned above. No special configuration or installation steps are required when deploying RSA IMG on VMware.

Installation Hardware Requirements for WebLogic

Note: This content replaces "Installation Hardware Requirements" in Chapter 1: "Introduction" in the *Installation on WebLogic Guide*. It includes updated information the memory requirements for the application server node.

The following hardware is required:

- Database machine. See the *Database Setup and Management Guide* for information on database machine requirements.

- WebLogic Application Server machine:
  - Memory - System meets the hardware requirements specified for the version of the WebLogic server used, with sufficient excess memory to meet the RSA IMG requirements. RSA recommends that you have the following minimum amounts of system memory available for the application SERVER NODE: 4GB for development environments, 8GB for production environments, and up to 32GB for environments with up to 300 concurrent users
  - tmp space: WebLogic deployment of RSA IMG requires 1GB of /tmp space, 2GB recommended.
  - The application server disk requires sufficient space for the deployed RSA IMG application and runtime data. While the application only requires 300MB, data collections can require several GB of space. 5GB is the recommended minimum. Actual size requirements for collections are dependent on your usage of RSA IMG.

Installation Hardware Requirements for WebSphere

Note: This content replaces "Installation Hardware Requirements" in Chapter 1: "Introduction" in the *Installation on WebSphere Guide*. It includes updated information the memory requirements for the application server node.

The following hardware is required:

- Database machine. See the *Database Setup and Management Guide* for information on database machine requirements.
- WebSphere application server machine:
  - Memory: System meets the hardware requirements specified for the version of WebSphere server used, with sufficient excess memory to meet the RSA IMG requirements. RSA recommends that you have the following minimum amounts of system memory available for the application SERVER NODE: 4GB for development environments, 8GB for production environments, and up to 32GB for environments with up to 300 concurrent users.
  - tmp space: WebSphere deployment of RSA IMG requires 1GB of /tmp space, 2GB recommended.
  - The application server disk requires sufficient space for the deployed RSA IMG application and runtime data. While the application only requires 300MB, data collections can require several GB of space. 5GB is the recommended minimum. Actual size requirements for collections are dependent on your usage of RSA IMG.

Verify Correct Database Configuration

Use the following commands to verify that the database used by RSA IMG has been configured correctly:

Verify that the import/export described in Deployment Summary is defined:

```
select * from all_directories where directory_name in ('AVEKSA_
EXPORTIMPORT_DIRECTORY');
```

Verify that the tables spaces described in Create Tablespaces exist:

```
SELECT * FROM USER_TABLESPACES WHERE TABLESPACE_NAME IN ('DATA_
256K','DATA_1M','DATA_25M','DATA_50M','INDX_256K','INDX_
1M','INDX_25M',
'INDX_50M');
```

Validate the XML package exists:

```
select username from all_users where username='XDB';
```

Validate the schemas described in exist:

```
select * from all_users where username in ('AVUSER', 'AVDWUSER',
'ACMDB');
```

Verify the timezone settings within the database. As sys dba, execute the following SQL statements:

1. SELECT DBTIMEZONE FROM DUAL;
2. SELECT avuser.Utilities_Pkg.Get_DBTimezone_Value FROM DUAL;

If the values from those two queries are not exactly the same, execute the following SQL statements:

1. alter database set time_zone='<value you got from the previous second query>';
2. shutdown immediate;
3. startup;

Verify that the value has in fact been updated to the value you have specified by executing the SQL statement:

SELECT DBTIMEZONE FROM DUAL;

Run the Installation Script

Note: This content replaces "Run the Installation Script" in Chapter 6: "RSA IMG Software Installation" in the Installation and Upgrade Guide. It includes content about why the installation script does not prompt for an ASM partition in a customer-supplied database installation scenario.

Procedure

1. Log on to the installation machine as the ‘admin’ user. (If you are doing a new installation, log on as the ‘root’ user.)
2. Run the installation/upgrade script.

   ```
   cd /tmp/aveksa/staging
   sudo ./install.sh
   ```

3. Accept the license agreement.

   Note: A series of installation prompts and installation validation output particular to your installation scenario appears.

4. If you have previously run install.sh and need to change the configuration, run the configuration script followed by the installation/upgrade script:

   ```
   cd /tmp/aveksa/staging/deploy
   sudo ./configure.sh
   ```

   Answer configuration questions, and then run:

   ```
   sudo ./install.sh
   ```

5. If you have not previously set the installation and package file locations, you will be prompted to specify the directories (both should default to the correct values).

   ```
   Where are the installation files located [/tmp/aveksa/staging]?
   Where are the package files located [/tmp/aveksa/packages]?
   ```

   Note: If you are upgrading, you can ignore any informational "could not find" warnings that may appear.

6. If you are doing a new software installation, you can choose to use the RSA-provide Oracle database (local only) or an your own Oracle installation (remote, customer-supplied).

   Note: RSA recommends that you choose N and install Oracle in a local database deployment scenario. This will install and configure Oracle on the appliance machine using a pre-defined Oracle configuration.

Local Database Scenario:

```
Is this a remote Oracle installation [N]? N
```

If you are doing a new or upgrade installation on an appliance, you may be prompted for the Oracle ASM partition. Enter the value determined during the pre-upgrade phase. See "Determining the Oracle ASM Partition" for more information. For the Dell R720 or the Dell 2900, this value is sdb1. For all other appliances, this value is sda3.

```
What is the Oracle ASM partition []? <ASM partition value>
```

If an installation has a database, you will be prompted to specify whether to retain and migrate the database:

```
An existing database was found. Do you want to keep the database [Y]?
```

If you choose to keep the database (Y), then you will prompted to specify whether to migrate the database. If not, the database will be destroyed and a new schema created.

```
Migration is necessary when upgrading. Do you want to migrate the
database [Y]?
```

Choose Yes. Data will be migrated during the installation process.

Note: Oracle is installed under the /u01/app/oracle/directory. If this is a non-appliance/non-ASM installation, the database files are created in the /u01/app/oracle/oradata/AVDB/ directory.

Remote Database Scenario:

Note: You are not prompted for the ASM partition in a soft-appliance, remote database installation scenario. ASM partitioning is germane only to installations on an RSA IMG appliance.

```
Is this a remote Oracle installation [N]? Y
```

If you choose Yes, proceed as follows.

You will be prompted to specify the remote Oracle database instance parameters. Consult the DBA who manages the database for parameter values:

```
What is the Oracle listener hostname []?
```

```
What is the Oracle listener port number []?
```

```
What is the Oracle SID []?
```

Is the Oracle Service Name the same as the Oracle SID []? (yes/no)

The following prompt allows you to specify an Oracle Service Name if it is different from the

Oracle SID.

What is the Oracle Service Name []?

```
What is the AVUSER password []?
```

```
What is the AVDWUSER password []?
```

```
What is the ACMDB password []?
```

```
What is the PERFSTAT password []?
```

If the remote database contains data, you will be prompted to migrate the database:

```
Migration is necessary when upgrading.  Do you want to migrate the
database [Y]?
```

Choose Yes. Data will be migrated during the installation process.

7. The installation begins. Wait until the following message appears:

   ```
   Installation Complete!
   ```

   If they appear, you can safely ignore the following error messages:

   ```
   insserv: warning: script 'init.ohasd' missing LSB tags
   ```

   ```
   insserv: Default-Start undefined, assuming default start runlevel(s) for
   script `init.ohasd'
   ```

8. Perform the post-installation firewall configuration procedure for servers running SUSE as described in "Firewall Configuration for SUSE" and for servers running Red Hat as described in "Firewall Configuration for Red Hat."
9. If you have saved SSL server or agent certificates that you would like to use, see "Back Up and Restore Default HTTPS Certificates."
10. Log on to RSA IMG to set the administrator password as described in "See Log on to RSA IMG," and verify correct installation as described in "Verify the Installation/Upgrade."
11. If you have previously backed up your database as described in Back Up the RSA-Supplied Database "Back Up the RSA-Supplied Database," then do the following:
    a. Restore the database after the installation. See "Importing AVUSER Schema/Data for a Database Restoration/Load" for more information.
    b. Migrate the database after the installation and after you have restored the database if you chose to not to migrate the database as prompted during the installation. See "Migrating the Database" for more information.

Configure Appliance Network Settings

You must assign or modify the network configuration information (ip address, host name and so on), configure domain name servers (DNS), and set the time zone in which the appliance is located. If you receieved a pre-configured appliance from RSA, refer to the Appliance Network Configuration sheet that shipped with the appliance for this information. You may still need, or want, to modify this configuration information.

Procedure

1. Login onto the appliance from the console using the "admin" account. If you received a pre-configured appliance from RSA, you can log onto the appliance using the iDRAC ip address listed on the Appliance Network Configuration sheet. Otherwise, do the following:
   a. At the login as prompt, enter admin.
   b. At the password prompt, enter changeme.

   Note: "changeme" is the default password for the "Admin" account. RSA recommends that you change the password after your initial login by issuing the `passwd <your new password>` command.

2. Modify the hostname of the appliance.
   a. Stop the RSA IMGservice. Enter

      ```
      service aveksa_server stop
      ```

   b. Start the Oracle database. Enter

      ```
      service aveksa_server startoracle
      ```

   c. Change the hostname. Enter

      ```
      sudo modifyhostname.sh <hostname.domain name>
      ```

      where `<hostname.domain name>` is the new name of the appliance.

      Important: The modifyhostname.sh script re-creates the server-side certificates with the new hostname, which affects AFX and all collector agents. If the installation includes the AFX module, you must re-create its client certificates to include the new hostname. For more information, see Change an AFX Server SSL Certificate in the Help. For all collector agents, you must generate new certificates for each agent, and then re-download and re-install the agent. For more information, see the topic Creating an Agent and the topic Viewing an Agent in the Help.

3. Stop the Oracle database. Enter

   ```
   service aveksa_server stoporacle
   ```
).

4. Configure the domain name servers.
   a. Enter
      `sudo setnameserver.sh <ns1> <ns2>`
      where <ns1> is the first name server and <ns2> is the backup name server.
   b. Verify the name server address. Enter
      `cat /etc/resolv.conf`
5. Configure the network settings for the system. Enter
   `sudo modifynetworksettings.sh <IP> <Netmask> <Gateway>`
   Where:
   - <IP> is the IP address of the appliance
   - <Netmask> is the Subnet mask
   - <Gateway> is the Network gateway
6. Set the time zone where your appliance is located. Enter
   `sudo setlocaltime <timezone>`
   where <timezone> is the abbreviation of a country and city in the same geographic location as the appliance. For a list of valid time zone abbreviations, see /usr/share/zoneinfo.
   For example, to set the time zone for an appliance located in New York, enter
   `sudo setlocaltime America/New_York`
7. Reboot the appliance. Enter
   `sudo reboot`
8. After reboot, you must restart Oracle database services and RSA IMG. Enter
   `sudo service aveksa_server startoracle`
   `sudo service aveksa_server start`
9. You can now log on to RSA IMG.

Create a Database User Password Profile

This section describes how to create a database profile for the users that connect to the database.

Oracle 12cR1 has a default password expiration of 180 days. If a database user password were to expire, RSA IMG would fail to connect to the database.

Important: If you choose to have a password policy that expires for the RSA IMG users, you will have to reconfigure the user database password settings when passwords expire. The sample file aveksa_db_password_lifetime.sql shows how to obtain the password lifetime information for the RSA IMG database users.

See the aveksa_sample_ora12_db_scripts.sql for installations using Oracle 12cR1 (12.1.0.2, 64-bit) script for examples on how to configure a database user password profile:

Enter the following command to create the profile:

```
Create Profile ACMPROFILE LIMIT PASSWORD_LIFE_TIME UNLIMITED;
```

Important: RSA does not require that you include the Oracle SYS user in the profile. The Oracle SYS user password, therefore, will expire at some point. RSA recommends you do.the following: change the password in the database and the application, reset the password to its current value, or include the SYS user in the profile.

About Diagnostic Window Resources

This window contains information about the heap dump file generated when a Java heap space has occurred.

- Initialization Warnings — Indicates that the RSA IMG server is not configured as recommended. A system configuration problem that causes a warning typically does not prevent the server from starting, but it certainly may portend potentially fatal run-times problems that can occur if the warning is not recognized and addressed.
- Database Logs — Lists and lets you access logs that can help you pinpoint system problems. Some or all of the following logs may be available depending on what actions have occurred with the system:

  aveksaServer.log - Provides information about the RSA IMG server execution. See for more information on managing aveksaServer.log settings.

  Note: If the aveksaServer.log indicates an “OutOfMemoryError” Java heap space error has occurred, RSA IMG automatically creates a heap dump file in the /home/oracle directory when it detects the error. The file format is: `acm-heap-dump-date.hprof.` This artifact provides a snapshot of memory of at a given point in time. This file may be requested by RSA Support for analysis.

  create.log - Provides information about interactions involved with deploying and/or migrating schema changes to the database.

  migrate.log - Provides information about database migration phases.

  patch.log - Provides information about script-driven hot fix installations.

reporting-user-synonyms.log - Provides information about updates to user synonyms in the avdwdb data source.

public-schema-synonyms.log - Provides information about updates to user synonyms in the acmdb data source.

- Collected Data — Indicates whether data files generated from data collections are retained in the system or deleted. You can edit this setting. See for more information.
- RSA IMG Statistics Report — Lets you generate, view, and download system statistics reports that provide information about your system implementation and that can help you pinpoint the causes of system problems. See for more information.
- Invalid Database Objects — Lists invalid database objects detected by the system. See for information on how to re validate the objects.

Migrating Custom Security Contexts

The migration process migrates all custom security contexts automatically, creates equivalent security contexts in the migrated environment and assigns the contexts to the users who had them before the migration.

The following naming conventions are used to name the equivalent security contexts:

- The Resource Name is the Object Type, as it was prior to migration.
- The Action Name is a combination of the security context's action and name as they appear in the filter. If no action name can be determined by the migration, sequential numbers are used to provide an action name for the security context.

For information about how your security contexts were migrated and renamed, see the following files in your installation:

- /aveksa.ear/aveksa.war/WEB-INF/MigratedSecurityContext.csv
- /aveksa.ear/aveksa.war/WEB-INF/MigratedSecurityDetails.csv

On an appliance, the aveksa.ear resides in /home/oracle/jboss/server/default/deploy/.

On a WebSphere or WebLogic installation, the aveksa.ear file resides in the location to which you deployed the .ear file.

Adding or Updating Custom Security Contexts Example 2

This example demonstrates how to create a new entitlement to grant access to multiple reports. Because this entitlement can be granted directly through an access request (or through a role if access request is not available), there will be no explicit columns.

```
SECURE_OBJECT_TYPE,NAME,ACTION,IMPLICIT_HAS_QUERY,IMPLICIT_BS_
CHANGE,IMPLICIT_BU_CHANGE,SCOPE_TABLE,SCOPE_FILTER Report Definition,Edit
Review Reports ACM48667,Edit,,,,V_LIST_REPORTS,"REPORT_NAME IN
('Revocation Report','Orphaned Users')"
```

Create the JDBC Data Sources

You must create the JDBC data sources RSA IMG uses to access the database. The steps for creating the JDBC data sources vary depending on whether your WebLogic installation uses a Standard Oracle Database or an Oracle RAC implementation. Review the steps before proceeding.

The following default RSA database user schema names are used in this task:

- RSA IMG user. The default name is AVUSER.
- RSA IMG reporting engine user. The default name is AVDWUSER.
- RSA IMG public database schema user. The default name is ACMDB.
- RSA IMG Statistics Report user. The default name is AVPERF. This user is required only if Oracle Statspack is installed on the database and you want to include Statspack data in Aveksa Statistics Reports. If you remove or disable Statspack on your database, remove the AVPERF data source and restart the database.

Note: If you created the database instance with non-default names, you must use the same user names and passwords when you create the JDBC data sources. See the *Database Setup and Management Guide* to ensure that the database instance meets the RSA IMG product requirements. To configure the JDBC data sources, you need the Oracle SID, Oracle listener hosts, Oracle listener port, and Oracle service name.

Create the following JDBC data sources required by RSA IMG:

- avdb
- avdwdb
- acmdb
- avperf
- Workflow (WPDS, WPDS2, WPDS3)

Procedure

1. Log on to the WebLogic console.
2. From the Services menu, select Data Sources.

3. Configure the data sources.
   - Click New to create each data source. From the New button menu, choose an option:
     - Generic Data Source for a non-Oracle RAC database.
     - Gridlink Data Source for an Oracle RAC database.
   - AVDB data source
     - Name: `AVDB`
     - JNDI Name(s): `jdbc/avdb`
     - Database Type: Oracle
     - Database Driver:
       Non-Oracle RAC: Oracle's Driver (Thin) for Instance connections
       Oracle RAC: Oracle's Driver (Thin) for RAC Service-Instance connections
     - Oracle RAC: Supports Global Transactions: Yes.
     - Oracle RAC: Select Enter complete JDBC URL.
     - Oracle RAC: Complete JDBC URL: `jdbc:oracle:thin:@//rac-ora-scan:1555/avdb`
     - Oracle RAC: Clear the flag for subscribing to FAN events.
     - Enter Connection properties to Oracle as specified in your Installation Worksheet.
     - Database Name: <*appropriate database SID*>
       Host Name: <*listener-hostname*>
       Port: <*database-listener-port*>
       RSA IMG Database User Schema Name: <*avuser*>
       Database password: <*password*>
     - Select Test Configuration.
     - Target: Choose the target server or cluster.
   - AVDWDB data source
     - Name: `AVDWDB`
     - JNDI Name(s): `jdbc/avdwdb`
     - Database Type: Oracle

- Database Driver:
  Non-Oracle RAC: Oracle's Driver (Thin) for Instance connections
  Oracle RAC: Oracle's Driver (Thin) for RAC Service-Instance connections
- Oracle RAC: Supports Global Transactions: Yes.
- Oracle RAC: Select Enter complete JDBC URL.
- Oracle RAC: Complete JDBC URL: `jdbc:oracle:thin:@//rac-ora-scan:1555/avdwdb`
- Oracle RAC: Clear the flag for subscribing to FAN events.
- Enter connection properties to Oracle:
  Database Name: *<appropriate database SID>*
  Host Name: *<listener-hostname>*
  Port: *<database-listener-port>*
  RSA IMG Database User Schema Name: *<avdwuser>*
  Database password: *<password>*
- Select Test Configuration.
- Target: Choose the target server or cluster.

- ACMDB data source
  - Name: `ACMDB`
  - JNDI Name(s): `jdbc/acmdb`
  - Database Type: Oracle
  - Database Driver:
    Non-Oracle RAC: Oracle's Driver (Thin) for Instance connections
    Oracle RAC: Oracle's Driver (Thin) for RAC Service-Instance connections
  - Oracle RAC: Supports Global Transactions: Yes.
  - Oracle RAC: Select Enter complete JDBC URL.
  - Oracle RAC: Complete JDBC URL: `jdbc:oracle:thin:@//rac-ora-scan:1555/acmdb`
  - Oracle RAC: Clear the flag for subscribing to FAN events.

- Enter connection properties to Oracle:
  Database Name: <*appropriate database SID*>
  Host Name: <*listener-hostname*>
  Port: <*database-listener-port*>
  RSA IMG Database User Schema Name: <*acmdb*>
  Database password: <*password*>
- Select Test Configuration.
- Target: Choose the target server or cluster.

- AVPERF data source
  - Name: `avperf`
  - JNDI name = `jdbc/avperf`
  - Database Type: Oracle
  - Database Driver:
    Non-Oracle RAC: Oracle's Driver (Thin XA) for Instance connections
    Oracle RAC: Oracle's Driver (Thin XA) for RAC Service-Instance connectionss
  - Oracle RAC: Select **Is this XA Driver**.
  - Enter connection properties to Oracle:
    Database Name: <*appropriate database SID*>
    Host Name: <*listener-hostname*>
    Port: <*database-listener-port*>
    RSA IMG Database User Name: <*perfstat_user*>
    Database password: <*perfstat_password*>
  - Select Test Configuration.
  - Target: Choose the target server or cluster.
- WPDS data source
  - Name: `WPDS`
  - JNDI Name(s): `WPDS`
  - Database Type: Oracle

- Database Driver:
  Non-Oracle RAC: Oracle's Driver (Thin XA) for Instance connections

  Oracle RAC: Oracle's Driver (Thin XA) for RAC Service-Instance connections
- Oracle RAC: Select Is this XA Driver.
- Enter connection properties to Oracle:
  Database Name: <*appropriate database SID*>

  Host Name: <*listener-hostname*>

  Port: <*database-listener-port*>

  RSA IMG Database User Schema Name: <*avuser*>

  Database password: <*password*>
- Select Test Configuration.
- Target: Choose the target server or cluster.

- WPDS2 data source
  - Name: `WPDS2`
  - JNDI Name(s): `WPDS2`
  - Database Type: Oracle
  - (Oracle RAC implementation): Select Is this XA Driver
  - Database Driver:
    Non-Oracle RAC: Oracle's Driver (Thin XA) for Instance connections

    Oracle RAC: Oracle's Driver (Thin XA) for RAC Service-Instance connections
  - Oracle RAC: Select Is this XA Driver
  - Enter connection properties to Oracle:
    Database Name: <*appropriate database SID*>

    Host Name: <*listener-hostname*>

    Port: <*database-listener-port*>

    RSA IMG Database User Schema Name: <*avuser*>

    Database password: <*password*>

- Select Test Configuration.
- Target: Choose the target server or cluster.

- WPDS3 data source
  - Name: `WPDS3`
  - JNDI Name(s): `WPDS3`
  - Database Type: Oracle
  - Oracle RAC implementation): Select Is this XA Driver
  - Database Driver:
    Non-Oracle RAC: Oracle's Driver (Thin XA) for Instance connections
    Oracle RAC: Oracle's Driver (Thin XA) for RAC Service-Instance connections
  - Oracle RAC: Select Is this XA Driver.
  - Enter connection properties to Oracle:
    Database Name: *<appropriate database SID>*
    Host Name: *<listener-hostname>*
    Port: *<database-listener-port>*
    RSA IMG Database User Schema Name: *<avuser>*
    Database password: *<password>*
  - Select Test Configuration.
  - Target: Choose the target server or cluster.

4. Save the configurations.
5. Edit the configuration for each data source:
   a. Go to the Connection Pool tab, expand the Advanced settings, then uncheck **Wrap Data Types**.

b. Configure the Set Maximum capacity value according to the following table:

Data Source	Maximum Capacity Value
AVDB	300
ACMDB	50
AVDWDB	50
WPDS	150 (Recommended minimum; heavy loads on workflows may require a higher setting.)
WPDS2	150 (Recommended minimum; heavy loads on workflows may require a higher setting.)
WPDS3	150 (Recommended minimum; heavy loads on workflows may require a higher setting.)

6. (Optional) Secure each data source with a security policy. You can enable security after installing RSA IMG.

   Note: The settings here are dependent on the users and groups defined in Create Security Realm Users and Groups.

   a. Select the new data source. (For example, AVDB) .

   b. Select Security tab > Roles sub-tab.

   c. Select New, and enter a security policy name: `acmUsers`

   d. Click OK.

   e. Select the Policies sub-tab.

   f. Select Add Conditions.

      - Predicate List: Select Role.
      - Role Argument Name: `acmUsers`

   g. Select Add.

   h. Select Finish.

   i. Select Save.

   j. Restart WebLogic.

Access Fulfillment Request (AFX)

This content replaces sections of the *Access Fulfillment Express Guide V2.9*.

Note: V2.9.x and V6.9.x are equivalent versions of AFX. The version number of AFX was updated to match the version number of RSA IMG.

Download an AFX Server Archive

For any non-RSA server on which you want install an AFX Server instance, you must first download an archive of an AFX Server that you want to install.

Procedure

1. Log in to RSA IMG.
2. Select AFX > Servers.
3. From the list of AFX Server configurations, select the server that you want to download.
4. From the AFX Server configuration detail page, click Download Server Archive.

   Note: It may take several minutes for the system to generate the AFX Server archive for download.
5. Specify the download location when prompted by the browser and save the AFX Server archive.
6. Install the archive. See Install the AFX Server Using an Archive Downloaded from RSA.

Change an AFX Server SSL Certificate

You must change the AFX server's SSL certificate when the certificate has been changed in RSA IMG. For example, if you updated the server.keystore certificate to SHA-256 you must update an AFX server's client certificate to SHA-256.

Procedure

1. Click the AFX menu and select Servers.
2. Select the server for which you want to update the SSL certificate.
3. Click Change Certificate.
4. Click OK in the Change Certificate window.
5. Click Download Keystore and save the client.keystore file on your computer.

6. Copy the client.keystore file to <AFX-home>/esb/conf
7. Restart AFX.

Known Issues and Limitations

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

Tracking ID	Description
ACM-56319	Adding a dynamic parameter of type boolean to a create account command is not supported in AFX.
ACM-52520	Only the Remove Change item is included in a request which was created to add and remove approles 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-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.
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 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 the system cannot be started (acm start) after the avuser password has been changed.

Tracking ID	Description
ACM-61342	The user is able to run forms that are disabled.
ACM-61779	For non-administrator user, listed and individual pages in the applications have different "Collect Data" behaviors, instead of being enabled or disabled everywhere.
ACM-61728	A user has entitlements to a deleted technical role. For a workaround, do not delete the role that is nested and remove the role from any hierarchy prior to deleting it. The un-nesting of the roles will properly clean up the entitlement.
ACM-62918	A report is exported as a jrxml file. When the file is imported, the jrxml query is imported but the default value text box for a bind variable is not rendered.
ACM-61958	The Group by User option in a reset password form does not display the user name.
ACM-63192	Under a user's Access tab, the technical role name is not displayed in the entitlement path of the group.
ACM-63488	A report result is not exported in .xls format on WebLogic 10.3.5. *Workaround*: Export the result in .csv format.