RSA Via Lifecycle and Governance

V7.0.0 Patch 1 Release Notes

Contact Information

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

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

Trademarks

License agreement

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 Via L&G 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

Copyright © 2015 EMC Corporation. All Rights Reserved.
Published in the USA.

Contents

Preface

This document lists what has changed and has been fixed, as well as known issues in RSA Via Lifecycle and Governance (RSA Via L&G). These *Release Notes* may be updated after the release.

This document is intended for RSA Via L&G administrators and users.

RSA Identity Management and Governance (IMG) has been rebranded to RSA Via Lifecycle and Governancee (RSA Via L&G).

Support and Service

RSA Via L&G Customer Support Knowledgebase	https://rsaportal.force.com/customer/_ui/-knowledge/ui/KnowledgeHome
RSA Via L&G Community	https://community.emc.com/community/connect/rsaxchange/rsa-img
RSA Customer Support information	www.emc.com/support/rsa/index.htm
RSA Customer Support email address	support@rsa.com
RSA SecurCare Online (SCOL)	https://knowledge.rsasecurity.com/ RSA SecurCare Online provides unlimited access to a wealth of resources on the Web, 24 hours a day. The secure system provides members access to a support knowledgebase, to download current platform patches and bug fixes, to sign up for notifications, to manage your support cases and more.

Download RSA Via L&G Software and Documentation

Customers can obtain the documentation and software for this release by downloading them from SecurCare Online (SCOL). (https://knowledge.rsasecurity.com)

To download the product documentation, including Release Notes, you can access the documentation page specific for the release by selecting the “Documentation” link at the top of the RSA Via Lifecycle and Governance product page.

To download the release software, after logging into SCOL, you can select the "My Support" link at the top of the page or the "Version Upgrades" link on the RSA Via Lifecycle and Governance product page. On either of these pages you will be presented with a list of products that you are entitled to based on the RSA products you have purchased.

My Support link: https://knowledge.rsasecurity.com/scolcms/mysupport.aspx

RSA Via Lifecycle and Governance product page:
https://knowledge.rsasecurity.com/scolcms/sets.aspx?product=rsa_img

RSA Via L&G Version Upgrades link:
https://knowledge.rsasecurity.com/scolcms/sets.aspx?product=rsa_img&_v=upgrades

Select the appropriate license link to access the software available for the products listed in the table below. If you do not have this license in your list of products, then please contact RSA Customer Support.

RSA Via L&G Products	
• Via Lifecycle • Via Governance • Via Governance/Lifecycle • Access Certification Manager • Access Request Manager • Access Fulfillment Express • SAP Adapter for AFX • Data Access Governance	• DAG Activity Monitor • IMG Soft Appliance • IMG R320 Appliance ACM/Governance • IMG R620 Appliance ACM/Governance • IMG R720 Appliance ACM/Governance • IMG R320 Appliance ACM/AFX/Lifecycle • IMG R620 Appliance ACM/AFX/Lifecycle • IMG R720 Appliance ACM/AFX/Lifecycle

Documentation Set

The RSA Via L&G documentation set consists of the following materials:

Document	Description
Release Notes	Describes what's new in the release, lists fixed issues, and lists known issues and workarounds. (PDF format)
Installation Guide	Provides information and instructions to install the product. (PDF format)
Upgrade and Migration Guide	Provides information and instructions for upgrading your product version and migration data. (PDF format)
Database Setup and Management Guide	Provides information and instructions on how to set up and manage a remote Oracle database for RSA Via L&G. (PDF format; also included in the online documentation.)
Online documentation (Help)	Contains all of the information needed to configure and use the

Document	Description
	product. (HTML5 format). **Note:** The online documentation HTML5 file set is also available as a zip file on SCOL. Download and unzip the file to your computer and click Launch_Help.htm to open the standalone version of Help.
Public Database Schema Reference	Provides information about the public view of the database schema. (PDF format; also included in the online documentation.)

Obtain the RSA Via L&G Documentation Set

The RSA Via L&G documentation set is available from RSA SecurCare Online (SCOL) on the Documents page (https://knowledge.rsasecurity.com/scolcms/documents.aspx?product=rsa_img&search=).

Collector and Connector Configuration Datasheets

Collector and connector configuration instructions are provided independently of the documentation set. Each configuration is available in a separate datasheet available from RSA SecurCare Online (SCOL) on the Collector and Connector Datasheets page (https://knowledge.rsasecurity.com/scolcms/set.aspx?id=10689). This allows RSA to provide you with the most up-to-date information without waiting for a new release.

These datasheets replace the configuration information in the Collectors Guide and the Connector Configuration Guide in the previous product version.

RSA Via Lifecycle and Governance Community

Use the RSA Via L&G Community to interact with your peers, other RSA Via L&G users, implementation partners and RSA consultants. You can post comments, ask questions, or answer questions that others have posted.

Whether you are a brand new customer of RSA Via L&G, or have been using the product for years, we believe that you'll find this private community to be valuable.

The RSA Via L&G Community is a private community and is only available to RSA Via L&G clients, partners and internal RSA staff.

Link: https://community.emc.com/community/connect/rsaxchange/rsa-img

Rules for Using the RSA Via L&G Community

- You must be a registered community user to participate in the community.
- Do not share any confidential information on the community.

- Keep all posts and interactions positive and civil.

Join the RSA Via L&G Community

Procedure

1. Register an account on the EMC Community Network (ECN): https://developer-content.emc.com/login/register.asp
2. Complete the RSA Via L&G Access Request form. This is a one-time only event that allows your account to access the RSA Via L&G Community. Please ensure you add in your partner or client name, so we can confirm who you are. https://developer-content.emc.com/email/request-rsa-img.htm

Once the Access Request form is submitted and received, the RSA Via L&G management team processes your request. This can take up to a week; we appreciate your patience. Once confirmed, you will receive a Welcome to the Community email from us with more instructions.

Install a Patch

Patches are cumulative. A product version patch includes all updates included in earlier patches for that version.

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

Procedure:

1. Download the following files available from RSA SecurCare Online at https://knowledge.rsasecurity.com:
   - RSA_Via_L&G_Release_Notes_<VersionNumber>.pdf
   - Aveksa_<VersionNumber>_P<PatchNumber>.tar.gz

   Note: If you have AFX installed on your system, download the updated connector templates in the connector.zip file or files appropriate for your AFX installation and import the templates into AFX after you complete the patch installation. For information on how to import connector templates, see the *Access Fulfillment Express* Guide.
2. Uncompress and untar Aveksa_<VersionNumber>_P<PatchNumber>.tar.gz.
   a. cd /home/oracle
   b. tar zvxf Aveksa_<VersionNumber>_P<PatchNumber>.tar.gz
3. Read the PatchInfo.txt file and the Patch-README.txt file in the Aveksa_<VersionNumber>_P<PatchNumber> directory created by Step 2.
4. Log in as root and run the patch.sh installation script in the directory created in Step 2:
   a. cd /home/oracle/Aveksa_<VersionNumber>_P<PatchNumber>
   b. sh patch.sh
5. When the patch script completes, restart RSA Via L&G. Enter

   ```
   acm restart
   ```

Note: For information on installing a patch on WebLogic or WebSphere, see the *Installation Guide*.

Release 7.0.0 Updates

Version	Date	Description
7.0.0 Patch 1	October 2015	Patch Release
7.0.0	August 2015	Major Release

Release 7.0.0 Patch 1

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

What's New in Release 7.0.0 Patch 1

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

Feature	What's New
Rules: Testing	The Provisioning - Termination and the Provisioning - Joiner/Mover rule definitions include a Test button. It allows you to test the rules just you can for User Access and SoD rules.
Rules	Tables that list users with violating access enable you to sort, group by, and search on custom attributes for those users.
User Access Review	The "Allow Group to be expanded to display access" option allows a reviewer to display the access provided by a group to a user. Reviewers can take action on the group, not selectively on the entitlements in the group. This enables the reviewer to determine whether to maintain or revoke the access provided by the group
Request Forms	RSA-provided forms are tagged as belonging to the "Default" category.

Fixed Issues in Release 7.0.0 Patch 1

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

Issue	Description
52579	
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-663107, 642394, 654876, 660592, 677237, 677764 ACM-54809	Some role entitlements are incorrectly removed during subsequent collections.
SF-731259 ACM-56794	RSA Via L&G 7.0.0 initial database setup fails with this error: "Unable to get database version.”
SF-727042 ACM-56813	A change request stalls in the approval node after processing over 1000 request items.
SF-657164 ACM-53336	Adding a node to workflow creates two instances of the node.
SF-596925 ACM-51030	The send email action is not executed for an attribute change rule.
SF-702306 ACM-55192	The Maintain and Revoke buttons in a review are unresponsive when French is designated as the default language for RSA Via L&G.
SF-	False AFX failures occur when adding or removing user accounts from groups in

Issue	Description
625568, 620646, 668423, 680413 ACM-52843, ACM-51871	Active Directory.
SF-627569 ACM-52088	Action buttons are disabled only for group owner reviewer when using the review results menu.
SF-725911 ACM-56545	Editing imported local entitlements changes entitlement names to entitlement raw names.
SF-643163 ACM-52537	Processing rules in one rule set processes all other active rules in other rule sets.
SF-690230 ACM-54602	The WebService cmd findEntitlements sortDirection parameter is not properly documented.
SF-711283 ACM-55815	Account collection taking an inordinate amount of time to complete after the account collector is configured to collect groups in addition to accounts.
SF-664551 ACM-54623	A user who rejoined an organization is not provisioned with the same entitlements he/she had prior to termination.
SF-710501 ACM-55667	A user who rejoined an organization is not provisioned with the role he/she had prior to termination.
SF-696638 ACM-54943	A "NullPointerException" error occurs when importing a rule definition that references a non-existent custom attribute.

Issue	Description
ACM-55414	Remediation workflows are not created for all user access rule violations.
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-705415 ACM-55485	Old change request identifiers are displayed for SoD rule names for violation remediation tasks under Admin > Workflows.
SF-678405, 700864 ACM-54309	A user who creates a change request is unable to cancel the request even though the request workflow is configured to allow cancellation.
SF-651276, 645804, 639819, 653846, 641001, 666533, 672358, 679297, 677862, 684959 ACM-52718	The Appliance tab on the Admin System page does not load.
SF-664872 ACM-53419	A change request does not close when the AFX workflow is configured with the "Create a job per group, grouping by user" setting.
SF-719788 ACM-56120	Infinite looping occurs after editing a role profile.
SF-690180 ACM-	A reviewer was unable to undo a sign-off on review items.

Issue	Description
54591	
SF-689461 ACM-54662	There is an issue with the "Set_ChangeItem_Category" procedure.
SF-700826 ACM-55870	An AFX fulfillment call after an approval did not occur.
SF-701486 ACM-55171	The Modify button is unavailable for users added to a review by a review refresh.
SF-697485 ACM-55072	Deleted user account mapping displays in the Reset My Password form.
SF-654610 ACM-53044	Role name changes from Role Set Name to Role Set Raw Name during the fulfillment process.
SF-698118, 681069 ACM-54989	An "Insufficient Privileges" error occurs when attempting to view a user's Request tab.
SF-689044 ACM-55312	Review email is not sent if one of the recipients has an invalid email address.
SF-692001 ACM-54672	When the name of an application role for a particular business source is changed, all equivalently named application roles for other business sources are changed as well.
SF-647629 ACM-52654	A problem occurs when attempting to create a business description for a set of application roles.
SF-698100	Saved report results are missing after an upgrade from v5.1.4 to v6.9.1.

Issue	Description
ACM-55120	
SF-691441 ACM-54738	(WebLogic) Changes to the user interface display settings are not reflected across nodes.
SF-697317 ACM-55069	Role definition reviews are generating change requests to revoke groups from users that are not members of the role.
SF-679345 ACM-54994	Asset Owner approval not working for entitlement of type account group. The approval is system-approved instead of being assigned to the asset owner.
SF-626239 ACM-51948	The Admin > System > Settings page shows inconsistent information when the database is remote and a local database has been imported.
ACM-54917	For the SoapWebService node, the proxy is not reset if cleared from the workflow node.
ACM-54431	When creating a new role and the fulfillment phase is set to group by user, the role remains in the Applied New state.
SF-680187 ACM-55131	A deleted role is included under a user's Access tab.
SF-694923 ACM-54944	Language in advanced search remains in English even when the language is changed in the Options link.
SF-705077 ACM-56002	Completed violating access remediation is indicated as pending.
SF-680826 ACM-54112	The MySQL connector does use the most current version of the jar file: mysql-connector-java-5.1.36-bin.jar
SF-19286	Import of Business Descriptions reports the Modified By field as AveksaAdmin even

Issue	Description
ACM-44975	if the import was performed by someone else.
SF-623248 ACM-52021	Time out and performance issues occur with change request approvals.
SF-692095 ACM-55130	Multi-app entitlement collections is taking over 18 hours to complete after installation of v6.8.1 p10.
SF-612345 ACM-51472	A request for an entitlement via an account for a user is rejected, yet the account appears under the user's Access tab.
SF-670181 ACM-53938	The AFX Salesforce connector did not support dynamic license variables.
SF-705986 ACM-55883	The Provisioning - Termination rule does not detect all terminated users.
SF-705698, 710766, 682951 ACM-55404	Cannot edit a SQL Execute node.
SF-702729 ACM-55196	An "ORA-01400: cannot insert NULL" error occurs when an SQL Execute node executes an insert on a not null type column in the database.
SF-21360 ACM-48408	There are duplicate breadcrumbs when drilling down in to requests, approval phase, and supervisor approval.
SF-679227 ACM-54820	An "HTTP/1.1 505 HTTP Version Not Supported" error occurs when attempting to select an application name that contains spaces from an access request form.

Issue	Description
SF-685415 ACM-54692	Users are not displayed under the Who Has Access tab for an application.
SF-545046 ACM-50059	A request submission question configured to display once is displayed multiple times.
SF-639987 ACM-52376	Password challenge questions are not localized for users' language choice.
SF-642293 ACM-53369	A Request form does not append the values in the non-visual fields when run to create an account.
SF-698511 ACM-55189	SSH Connector does not work when there are special characters in data from 6.9.1 P02.
ACM-53118	Some Aveksa application entitlements are not providing the privileges they are designed to provide.
ACM-55838	(WebSphere and WebLogic only) An error occurs when a unique ID value is used to search for a user in the Users table.
SF-696326 ACM-55082	Log in from an AD authentication source takes an inordinate amount of time.
SF-722232 ACM-56276	A requestor cannot proceed through a form if a required field that does not meet the display criteria is not displayed.
SF-538188 ACM-49730	The Requested On timestamp changes each time an approver clicks the Perform button for an approval.
SF-717733 ACM-56045	A null variable in email generated from a workflow displays as ' ' characters.

Issue	Description
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-731761 ACM-56814	A role's Analytics tab shows missing entitlements not actually missing after entitlement collection is run.
SF-728873 ACM-57591	Monitoring policies do not allow the user designated as the monitor to view account change requests for accounts.
SF-742983 ACM-57810	Escalation Workflow reassigned to the wrong Data Owner when a request contained approvals for more than one entitlement, and those entitlements had different Data Owners.
SF-730782 ACM-57594	In Requests > Request page, unable to edit a Change Request Workflow.
SF-732768 SF-737557 ACM-56957	In an approval workflow, group by selections does not work correctly. A single request appears twice in the group owner's approval list and sends two emails to the Group Owner.
SF-730334 ACM-56776	After a system restart, a change request is processed by the wrong workflow.
SF-728492 ACM-56703	In Requests > Configuration > Request Forms tab, when selecting and running a form, the User Picker - User filter using "avform" variable resets to "None."

Issue	Description
SF-729843, 743321, ACM-56797	After submitting review items for sign-off, the Maintain and Revoke buttons remained enabled. These buttons are now "greyed-out" and not available when the review is submitted.
SF-730311 ACM-56718	Requests are getting stuck in Open state, after adding an entitlement to a role. This issue was fixed so that such requests now move forward to the Approval stage.
SF-671161 ACM-54544	The "Entitlements Require Accounts" settings for applications are not exported in metadata.
SF-622727 ACM-52249	There is no rule escalation workflow that initiations revocation of violating access if that access is not remediated by a particular due date. For more information, see What's New in Release 7.0.0 Patch 1.
SF-741059 ACM-57735	The following workflow error occurs: "ORA-06512: at "AVUSER.ACCESS_REQUEST_PKG", line 314."
SF-659351, 710259, 714047 ACM-53308	Workflow error occurs when evaluating a SQL node that is not in the processing path.
SF-739244 ACM-58274	A multi-app account collector and a multi-app entitlement collector are granting access to other application accounts if the account name is the same.
SF-751429, 756354 ACM-58885	When using WebSphere JAAS and Via L&G Authentication, cannot authenticate to Active Directory on port 636.
SF-749097 ACM-	After installing 6.9.1.07, the installation seems to have completed, but after restarting services, the RSA Via L&G user interface is not starting.

Issue	Description
58493	
SF-759615 ACM-59522	Role change request is created with wrong requestor.

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-55216	A "Caught SQLException: ORA-00904: "STATE": invalid identifier" error occurs when a report is run.
ACM-55664	Entitlements of the type, Global Role, cannot be added to a role in a role set even though the Entitlement Rule setting for the role set allows that entitlement type to be added to the role.
ACM-56022	An entitlement collector from an AD source collects account-to-entitlement relationship is collected twice
ACM-52520	Only the Remove Change item is included in a request which was created to add and remove application roles for a user.
ACM-52471	When the Back button is selected in a request form, previously entered field values are not refreshed.
ACM-51564	The name of a reviewer selected in review definition disappears. It reappears in the review definition when the definition is subsequently saved and then re-opened for editing.
ACM-51562	Inconsistent bulk and single account review action results occur.
ACM-48298	When the "Allow Manual Activity to Complete before Collection" feature is enabled, the entitlement or application role is not added or removed.
ACM-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

Tracking ID	Description
	Web Service connector capabilities instead of a message that indicates the cause of the error.
ACM-54603	The error message displayed in the log file should be more detailed when RSA Via L&G cannot be started (acm start) after the avuser password has been changed.
ACM-57362	Any remote agents that you install must be running the same version of the Java OpenJDK that is running on RSA Via L&G. The current supported version is

Post-Upgrade Cleanup of the /home/oracle Directory on an Appliance

After an appliance or software appliance upgrade completes, the /home/oracle directory contains the following two items that are no longer used by the upgraded system:

- A “jboss” symbolic link, which points to a directory (/home/oracle/jboss-4.2.2.GA) that is removed as part of the upgrade.
- The jboss-4.2.2.GA.tgz file, which contains an archived backup of the jboss-4.2.2.GA directory. This archive may contain files, for example log files or SSL certificates, that you may want to retain.

Procedure

1. Delete the “jboss” symbolic link. As the root user or the oracle user, enter

   ```
   unlink /home/oracle/jboss
   ```
2. Back up the jboss-4.2.2.GA.tgz file to a system other than the appliance.
3. Delete the jboss-4.2.2.GA.tgz file. As the root user or the oracle user, enter

   ```
   rm -rf jboss-4.2.2.GA.tgz
   ```

Help Supplement

This section includes RSA Via L&G v7.0 product content that is outdated in or not in Help.

Feature	Content
Cancel a Running Task: Reviews	The ability to cancel a running data collection task also applies to review generation and review refresh run tasks. For more information, see "Canceling a Running Data Collection Processing Task" in Help.
Create Topic and Object Dashboards	You can create topic and object dashboards to provide users with information in report and chart formats. **Procedure** 1. Click the Admin menu and select Dashboards. 2. Select the Topic Dashboards or Object Dashboards tab. 3. Click Create Dashboard. 4. Configure the dashboard, and then click OK. For more information, see "Create a Welcome Dashboard" in Help.
Editing a Workflow in Internet Explorer 11	If you have difficulties editing a workflow, activate Enterprise Mode for the browser. **Procedure** 1. Click Tools. 2. Toggle Enterprise Mode (checked) If you do not have the Enterprise Mode option under Tools, use this alternative method. **Procedure** 1. Click Tools. 2. Select F12 Developer Tools. 3. Select the Emulation icon (monitor and cell phone). 4. Select a mode lower than Edge.
Outdated Help Topics: "View Aveksa Application	Both topics incorrectly cite the following navigation path to the User Privileges Tab option: Admin > System >Settings

Feature	Content
Role Privileges for a User" and "Managing RSA Via L&G Application Role Grants Directly"	The correct navigation path to the option is listed as follows: Admin > User Interface
Outdated Help Topic: "Prepare the Oracle Database Instance"	For up-to-date content, see the "Prepare the Oracle Database Instance" below.
Outdated Help Topic: "Configuring the Web Service Plug-In"	For up-to-date content, see the "Configuring the Web Service Plug-In" topic below.
Outdated Help Topic: "About External Form Validation"	For up-to-date content, see the "About External Form Validation" topic below.
Help Topic: "Attribute Change Logging"	For up-to-date content, see the "Attribute Change Logging" topic below.
Missing Help Topic: "Configure a Two-Step Remediation Rule Action"	For content, see the "Configure a Two-Step Remediation Rule Action" topic below.

Prepare the Oracle Database Instance

Do the following on the database server:

1. Create or identify the instance name that is going to be used.
2. Ensure that the database instance uses the Unicode (AL32UTF8) character set.

   You can validate the character set by simply running the following SQL:

   ```
   select * from NLS_DATABASE_PARAMETERS where parameter='NLS_CHARACTERSET';
   ```

   Output: `NLS_CHARACTERSET AL32UTF8`

   RSA Via L&G will fail to start if this character set is not set for the database instance.

This character set is not the default when configuring Oracle. NLS_LENGTH_SEMANTICS is required to be BYTE, do not change this setting to CHAR.

Note: The following steps in this section assume that your database is initialized using an spfile and not a pfile. To determine if your database is using a pfile or an spfile, you can run the following commands via SQL*Plus. If the first command returns a value for "ifile", then the this value is the name and location of the pfile for your system. If an "spfile" value is found, then this is the name and location of the spfile for your system.

```
show parameter ifile

show parameter spfile
```

One of these commands returns a value.

Convert the a pfile into an spfile if your system is using a pfile. For example:

```
shutdown immediate;

startup pfile=<ORACLE_HOME>/dbs/init<ORACLE_SID>.ora

create spfile='<ORACLE_HOME>/dbs/spfile<ORACLE_SID>.ora' FROM pfile='<ORACLE_
HOME>/dbs/init<ORACLE_SID>.ora';

shutdown immediate;

startup;
```

3. Configure memory management settings for Oracle.

	ASMM		AMM	
Sys Mem	**SGA**	**PGA**	**Mem Target**	**Mem Target Max**
=>32G	8589934592	8589934592	16384M	17408M
=>16G	4294967296	4294967296	8192M	8704M
=>8G	2097152000	2097152000	4096M	4352M
<8G	1325400064	466616320	1709M	1709M

Setting ASMM Values:

a. Determine the memory allocation by running the following SQL:

```
show parameter sga_max_size;
show parameter sga_target;
show parameter pga_aggregate_target;
```

b. Enter recommended values in the init*.ora file as required using values from the table above:

```
alter system set pga_aggregate_target=<pga_value> scope=both;
alter system set sga_max_size=8589934592 scope=spfile;
shutdown immediate;
startup;
alter system set sga_target=<sga_value> scope=both;
```

c. Setting AMM Values:

```
ALTER SYSTEM SET MEMORY_MAX_TARGET = <mem_max_target> SCOPE = SPFILE;
shutdown immediate;
startup;
ALTER SYSTEM SET MEMORY_TARGET = <mem_target> scope = both;
ALTER SYSTEM SET SGA_TARGET = 0 scope = both;
ALTER SYSTEM SET PGA_AGGREGATE_TARGET = 0 scope=both;
```

d. The database server must have /dev/shm configured to support the amount of memory that Oracle will allocate (memory_max_target). To check the settings, log on to the database server and run the command:

```
df -h /dev/shm
```

e. The database server should use what is "Avail."

```
Filesystem Size Used Avail Use% Mounted on
tmpfs 18G 176M 18G 1% /dev/shm
```

4. Configure adequate space for all system tablespaces (see Configure Undo, Temp, and Redo Sizes).

5. Make sure that the database instance is configured with the XML_DB package. You can verify that XML DB has been installed by simply running the SQL below:

```
select comp_name from dba_registry where comp_name like '%XML%';
```

You should see results like the following:

```
COMP_NAME
```

Oracle XML Database

If this package does not exist, it can be installed with the database configuration assistant (dbca) or manually by executing the instructions found in the Oracle documentation at the following location:

http://download.oracle.com/docs/cd/B19306_01/appdev.102/b14259/appaman.htm#CACIBCBA

6. Specify the following database optimizer settings:
   - OPTIMIZER_INDEX_COST_ADJ — Lets you tune optimizer behavior for access path selection to make the optimizer more or less prone to selecting an index access path over a full table scan.
   - OPTIMIZER_INDEX_CACHING — Lets you adjust the behavior of cost-based optimization to favor nested loops joins and IN-list iterators.
   - OPTIMIZER_ADAPTIVE_FEATURES — Enables or disables all of the adaptive optimizer features

   Run the following commands to specify the optimizer settings:

   alter system set optimizer_index_cost_adj=30 scope=both;

   alter system set optimizer_index_caching=50 scope=both;

   alter system set optimizer_adaptive_features = false;
7. Modify the value of the cursor sharing parameter `cursor_sharing`, which determines which kinds of SQL statement can share the same cursors. Run the following command:

   alter system set cursor_sharing=force scope=both;
8. Validate that database requirements are reflected in your base Oracle startup by validating the spfile used by your database instance. Use this command:

   SELECT NAME, Value FROM gv$parameter order by name
9. Configure the database to accommodate a minimum of 600 sessions and 400 processes by running the following commands:

   alter system set sessions=600 scope=spfile;

   alter system set processes=400 scope=spfile;

   If your database will be serving multiple application server nodes, multiply the session and process numbers by the number of nodes.
10. Configure the log_buffer setting to 200 MB and the log_checkpoint_interval setting to 180 MB:

    alter system set log_buffer=209715200

    alter system set log_checkpoint_interval=188743680

The default settings for these support online transactional processing (OLTP) systems and not Data Warehousing systems. The larger settings are required to support data collections (which are more Data Warehouse style activities) by RSA Via L&G.

11. Configure the creation of deferred segments for tables to false. This is required for the Oracle 12c R1 Enterprise version.

    alter system set DEFERRED_SEGMENT_CREATION = FALSE

12. Restart the database server.

Configuring the Web Service Plug-In

Important: This only applies to users using the on-premise RSA Via L&G application.

This section describes how to configure the inbound interface plug-in.

Plug-in framework files include:

- aveksa-plug-ins.xml
- lib/UserAttributeChangeWebService.jar

To configure the aveksa-plug-ins.xml file:

1. Shut down the application server.

   sudo service aveksa_server stop

2. Run the customizeACM.sh script to extract the aveksa.ear file. For information on running the script, see "Customize RSA Via L&G" in the *Installation Guide*.
3. Go to the following directory of the extracted EAR file:

   /aveksa.war/WEB-INF/plug-ins/UserAttributeChangeWebService

4. Open the aveksa-plug-ins.xml file with a text editor.
5. Enable the plug-in by changing the following element to true:

   <enabled>true</enabled>

6. Configure the following elements:
   - id-attribute — Provide the internal name of the database column that should be searched for the value passed as the ID element on the request from Novell IM to update an attribute in ACM. For example: Unique_ID.

- attribute-name-mapping — Provide the name of the source attribute (external-name) that is mapped the corresponding attribute (internal-name) for a user in RSA Via L&G. Configure an element for each attribute mapping.

  For example:

  ```
  <attribute-name-mapping>
      <internal-name>DEPARTMENT</internal-name>
      <external-name>dept</external-name>
  </attribute-name-mapping>
  <attribute-name-mapping>
      <internal-name>TITLE</internal-name>
      <external-name>title</external-name>
  </attribute-name-mapping>
  ```

- run-rule — Provide one or more rules that the inbound interface executes to initiate the attribute change in RSA Via L&G.

  For example:

  ```
  <run-rule>Attribute Change Rule </run-rule>
  <run-rule>Global Role User Constraint Difference Rule </run-rule>
  <run-rule>Global Entitlement Rule </run-rule>
  ```

- run-all-rules — Specify this element to run all available rules by default.

  For example:

  ```
  <run-all-rules> </run-all-rules>
  ```

  Note: You cannot specify run-rule and run-all-rules elements in the same configuration. If you do not specify the run-rules element or the run-all-rules element no rule is executed for a request.

7. Run the customizeACM.sh script to rebuild and deploy the aveksa.ear file. For information, see "Customize RSA Via L&G" in the *Installation Guide*.
8. Restart the application server.

   ```
   sudo service aveksa_server start
   ```

About External Form Validation

External form validation comprises both field and form validation.

Field Validation

For field validation, the URI is called with three parameters:

- name — The Variable Name defined on the field.
- question — The Question defined on the field.
- value — The value for the name/question to test.

If there is an error, the error should reference the question. For no error, the response should be empty (whitespace is ignored). If the URI does not include the schema, hostname, and port, these are added.

For example, if you have a demo.war with validatephone.jsp script that validates a phone number provided by a form user in response to question on the form and this application is accessible on the same server as "/demo," then the Validation URI should be /demo/validatephone.jsp, and validatephone.jsp would look similar to the following:

```
<%
        String name = request.getParameter("name");
        String question = request.getParameter("question");
        String value = request.getParameter("value");
        if (!value.matches("[(][0-9][0-9][0-9][)] ?[0-9][0-9][0-9]-[0-9][0-9][0-9][0-9]")) {
        out.println("Invalid phone number for " + question + ", expected (###) ###-####");
}
<%
```

Form Validation

For form validation, the URI is called with two parameters for each field:

- value.variable — The name contains the value.
- question.variable — The name contains the question.

Form level validation also includes the attributes of key objects:

- avform.application.<attributes> — The associated application object (if application form)
- avform.businessunit.<attributes> — The associated business unit object (if business unit form)
- avform.requestor.<attributes> — The logged in user making request
- avform.users[index].<attributes> — The target users (only index 0 if there is one user)

Because of the large number of parameters, this request uses the POST method. Attributes that have null values do not have their parameters added. If there is an error, the error should take the form:

- error.variable-name1=error message
- error.variable-name2=error message
- error=A global error message, if one is needed

For example, if you have a demo.war with validateform.jsp and this application is accessible on the same server as "/demo," then the Validation URI should be /demo/validateform.jsp and validateform.jsp would look something like:

```
<%@ page import="java.util.Enumeration" %>
<%@ page import="java.util.HashMap" %>
<%
        HashMap<String, String> values = new HashMap<String, String>();
        HashMap<String, String> questions = new HashMap<String, String>();
        // Make the parameters and questions easy to access
                for (Enumeration e = request.getParameterNames(); e.hasMoreElements();) {
                String name = e.nextElement().toString();
                String value = request.getParameter(name);
                if (name.startsWith("value.")) values.put(name.substring(6), value);
                if (name.startsWith("question.")) questions.put(name.substring(9), value);
}
if (!values.containsKey("something else")) {
        out.println("error=Where is the something else field!");
        return;
}
if (!values.get("something else").contains("Important")) {
        out.println("error.something else=Where is the \"Important\" in " + questions.get("something
        else"));
        return;
}
%>
```

External Validation Warnings

- If any form validation request takes more than 3 seconds, a warning is displayed in the log output.
- If the total external validation request takes more than 3 seconds. a warning is displayed in the log output.
- If the total external validation time takes more than 3 seconds, a warning is displayed in the log output.

All external validation is logged with the category com.aveksa.gui.ExternalValidation.

Setting Up Your Own WAR

If you are using WildFly, you can create a directory on the application server such as demo.war in /home/oracle (or any other directory of your choice). Any file that you put in that directory is available through the application server with a URL like https://hostname/demo/file-in-demo.war. The name "demo" was derived from "demo.war". This can contain form selectors, field validations, form validations, and list control data sources.

Run this command from the directory where demo.war is located and while WildFly is running to deploy your demo.war in WildFly:

```
${AVEKSA_WILDFLY_HOME}/bin/jboss-cli.sh -c --command="deploy demo.war --force"
```

Attribute Change Logging

Important: This only applies to users using the on-premise RSA Via L&G application.

Each successful attribute change will have a log entry written using Log4J under the category audit.com.aveksa.server.webservices.UserAttributeChangeWebService which is written to /home/oracle/wildfly/standalone/log/aveksaServer.log by default. The format of a log entry is:

changed ‘attribute’ to ‘value’ on user ‘user-id’

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 Via L&G 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.