RSA Identity Management and Governance
V6.9 Service Pack 1 Patch 3 Release Notes

Contact Information

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

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

Trademarks

RSA, the RSA Logo, and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to **www.emc.com/legal/emc-corporation-trademarks.htm#rsa**.

License agreement

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

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

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

Third-party licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed by launching the RSA 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.

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

Contents

Preface

This document lists what has changed and fixed, as well as known issues in RSA Identity Management and Governance (IMG). These *Release Notes* may be updated after the release.

This document is intended for RSA IMG administrators and users.

Support and Service

Customer Support information	**www.emc.com/support/rsa/index.htm**
Customer Support email address	**support@rsa.com**
RSA SecurCare Online (SCOL)	**https://knowledge.rsasecurity.com/** RSA SecurCare Online (SCOL) 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 IMG Software and Documentation

You can download RSA IMG software and documentation from the RSA SecureCare Online (SCOL) site. Once you log on to SCOL and access the correct page, you are presented with a list of products that you are licensed to download. If you do not see a license for RSA IMG in the list of available products, contact RSA Customer Support.

Procedure

1. Log on to SecurCare Online using your SCOL account user name and password.
2. Select the "My Support" link at the top of the page or the "Version Upgrades" link on the Identity Management and Governance product page.
3. Select the appropriate license link to access the available Identity Management and Governance software downloads.

IMG Product Selected	Available Software Files
Access Certification Manager	ACM-WebLogic-<Product_Version>.tar ACM-WebSphere-<Product_Version>.tar
IMG Software Bundle	aveksa-<Product_Version>.tar.bz2
IMG R320 Appliance (ACM) IMG R320 Appliance (ACM & AFX) IMG R620 Appliance (ACM) IMG R620 Appliance (ACM & AFX) IMG R620 Appliance (ACM) IMG R620 Appliance (ACM & AFX)	aveksa-<Product_Version>.tar.bz2 rsaimg_updater_<Product_Version>.tar.bz2
Access Fulfillment Express	AFX-<Product_Version>-Connector-Converter.zip AFX-<Product_Version>-Standard-Connectors.zip
SAP Adapter for AFX	AFX-<Product_Version>-Premium-Connectors.zip

RSA Identity Management and Governance

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

- Access governance - Governs who has access to what applications and data resources based on job requirements and organization-wide security polices.
- 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 3	May 2015	Patch Release
6.9.1 Patch 2	April 2015	Patch Release
6.9.1 Patch 1	March 2015	Patch Release
6.9.1	March 2015	Service Pack Release

Release Notes

The RSA IMG *Release Notes* contains the following information about each release:

- What's New - new features and enhancements, and updates to existing features.
- Fixed Issues - list of fixed reported issues.
- Known Issues - list of known issues in the product as of the latest release (this includes service packs and patches).

The full documentation set is not updated for service packs and patches. The full set of information for new features and enhancements is available in the Documentation Supplement section of the *Release Notes*. The Documentation Errata section includes corrected topics that are to replace previously released topics in the documentation set.

Information in the *Release Notes* is organized by release (major, minor, service pack, and patch), with the most recent release at the beginning of the document.

The *Release Notes* may be updated after the release. Check SCOL for the latest version of the *Release Notes*.

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 an earlier 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_IMG_Release_Notes_<VersionNumber>.pdf
   - Aveksa_<product version>_P<VersionNumber>.tar.gz
2. Uncompress and untar Aveksa_<VersionNumber>_ P<VersionNumber>.tar.gz.
   a. cd /home/oracle
   b. tar zvxf aveksa-_<VersionNumber>_P<VersionNumber>.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. Run the patch.sh installation script in the Aveksa_<VersionNumber>_ P<PatchNumber> directory created by Step 2 as root.

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

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 is completed.

Feature	What's New
	• 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 MyAccessLive 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.

Tracking ID	Description
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.
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.

Feature	What's New
Workflows	The Email tab under Properties for a "Request Completed" 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.

Tracking ID	Description
SF-22004 ACM-48648	A database deadlock stalls a user access review.
SF-655400/658664/669134 ACM-52861	A reviewer is unable to access a review from a link in notification email because of "insufficient privileges."
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.

Tracking ID	Description
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 ACM-53267	An AirWatch collector fails with a "JSONObject Password not found" 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

Feature	What's New
	the application has been removed.
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.

Feature	What's New
	Define a reviewer example: 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.

Tracking ID	Description
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 ACM-51196	When the Back button in a form is selected by a user, the default value for the 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	A role owner loses role privileges when the owner changes the owner

Tracking ID	Description
ACM-51769	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.
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	An account is created for a user entitlement request despite the fact that the request was canceled in the approval phase.

Tracking ID	Description
ACM-51427	
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.
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	A provisioning joiner/mover rule is not suggesting business roles when it is configured to suggest roles.

Tracking ID	Description
ACM-49820	
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*.

Scenario	Action
	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 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

Feature	What's New
	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 "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.

Feature	What's New
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 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

Feature	What's New
	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: Customizable Password Reset Prompt Text	The password management "External Password Reset information 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.

Feature	What's New
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.
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.

Feature	What's New
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 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

Feature	What's New
	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, 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.

Feature	What's New
	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 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

Feature	What's New
	• 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. 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

Feature	What's New
	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.

Tracking ID	Description
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.
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.

Tracking ID	Description
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, 49290, 49291, 49292, 49293, 49294, 49295, 49296, 49297, 49104	Users with View All entitlements can complete the following tasks: • cancel a request • 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	Suggested entitlement is not shown in the Default Provisioning Form.

Tracking ID	Description
ACM-48583	
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.
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	An advanced supervisor filter in a request form is not saved.

Tracking ID	Description
ACM-48963, 47686	
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.
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.

Tracking ID	Description
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.
SF-14934, 17875 ACM-37418	The afxinstall script fails if you do not provide a fully qualified installation directory path.
SF-616383	No documentation available on how to install/upgrade a database driver user for collections.

Tracking ID	Description
ACM-46123	
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 ACM-46895	An ORPHAN_DATE column is not included in the T_AV_ ACCOUNTS public schema objects.

Tracking ID	Description
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	Various operational issues observed using RSA IMG on Internet

Tracking ID	Description
ACM-50549	Explorer v9.
SF-18814 ACM-44285	Form fields are displaying question mark ("?") characters.
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	There are unnecessary check boxes in the table in the Manage

Tracking ID	Description
ACM-49811	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.
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.

Password Management Settings

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.
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

Field	Description
	password reset by providing one or more attribute values to confirm their identity. **Note:** 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 knowledge of the REST 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. Right-click the REST Web Service Node and select Properties.
2. Configure the following tabs:

Tab	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

Tab	What You Enter
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. Click OK.

Configure a SOAP Web Service Node

Before You Begin

- You must have knowledge of the SOAP 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. Right-click the SOAP Web Service Node and select Properties.
2. Configure the following tabs:

Tab	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

Tab	What You Enter
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. Click OK.

Reassign Rule Violation Remediation Tasks in Bulk

Users whose privileges include Rule: Admin can reassign a group of 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.

Procedure

1. Click the AFX menu and select Servers.
   The Servers window appears.
2. Select the server for which you want to update the SSL certificate.
   The Server details window appears.
3. Click Change Certificate.
   The Change Certificate window appears.
4. Click OK. RSA IMG generates a new SSL certificate and associates it with the server.
5. Click Download Keystore.
6. Save the client.keystore file to <AFX-home>/mule/conf
7. Restart AFX.

Note: If you had previously installed this AFX server, until this step is executed, the existing installation with the old server SSL certificate will not be able to communicate with RSA IMG.

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. Security is implemented using Open Web Application Security Project (OWASP) Java HTML sanitization libraries. (See https://www.owasp.org for more information.)

  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 "Allowed Markup Input Whitelist" 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.
- MyAccessMobile 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 "Requesting a User Password Reset After a Failed Login Attempt" 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. See "Manage Login Account Password Reset Challenge Questions" in the *Access Request Manager Guide* for more information. 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 a “User Lockout” admin error. See "Viewing and Managing Admin Errors" for information on viewing admin errors and configuring system-generated email notification of admin errors for system administrators. Require secure connections from browsers: 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 "Managing Account Password Reset Implementation" for more information on password security features.

Option	Description
Server Certificate Store for Agent SSL Connections	Lets you download the server.keystore file.
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 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.

Option	Description
Web Services Session	Lets you specify timeout and expiration parameters for MyAccessMobile sessions. Session inactivity timeout: Lets you specify the amount of time a MyAccessMobile session is inactive before it expires. For example, a user has exited a 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. See "Setting Up RSA IMG for MyAccessMobile Access" for more information.
Security	Lets you specify security settings for MyAccessMobile. The Allow mobile app to save username setting lets you specify whether MyAccessMobile prompt users to save their login user names. The default setting is No. The Require secure connections setting 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. See "Setting Up RSA IMG for MyAccessMobile Access" for more information. See "Managing Operations Using the Web Services API" for more information on web services commands.

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

State	Description
	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 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.

State	Description
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 SecureCare Online at https://knowledge.rsasecurity.com. 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

Note: This topic replaces the existing topic in the *RSA IMG Installation Guide V6.9* .

You must download operating system installation files to a computer (not the appliance) from the RSA SecureCareOnline (SCOL) site and create the installation DVD that you will use to install the operating system on the appliance.

Procedure

1. Log in to the SCOL site and download the image:

   `dvd-SLES-11SP3-ACM-6.9.1.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
  - 8445: 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

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

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 Aveksa 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 "Create User Schemas" 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 remote 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).

   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 "Export the AVUSER Schema/Data for a Database Backup," 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 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. 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**.

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.

Request Commands

Note: This content replaces "Request Commands" in Chapter 24: "Managing Operations Using the Web Services API".in the *Administrators Guide*. It includes the complete set of request commands available from Web Services.

Command	Description
cancelChangeActivity	Used to cancel an assigned activity that is not completed. UI Equivalent: Requests - Activities - <Activity> - Cancel

Command	Description
cancelChangeRequest	Used to cancel a change request. UI Equivalent: Requests - <Request> - Cancel
createChangeRequest	Used to generate change requests. UI Equivalent: Requests - Create Request
createRequestsByOwner	Used to generate change requests for a review by a review owner. This command is ignored for reviews configured to automatically generate requests. UI Equivalent: Reviews - Results - <Review Result> - Change Preview tab - Create Change Requests
findApprovals	Used to search for approvals for the user specified by a valid session token provided as an input parameter.
getApprovalDetails	Used to get the details of a particular approval. The user specified by the valid session token provided as an input parameter must have access to the requested approval.
getApprovalsForUser	Used to get approvals for the user specified by the valid session token provided as an input parameter.
getChangeRequestStatus	Used to o determine the status of a given change request. UI Equivalent: Requests - <Request>
getFormToken	Used to generate a session specific form token representing a form name. This is required for security.
getRequestItems	Used to get information about the changes encompassed by a particular change request or approval. The user specified by the valid session token provided as an input parameter must have access to the requested approval.
performApproval	Used to accept or reject an approval. The user specified by the valid session token provided as an input parameter must be allowed to perform the requested approval.

Create a Database User Password Profile

Note: This content replaces "Create a Database User Password Profile" in Chapter 2: "Set Up the Database" in the *Database Setup and Management Guide*. It includes information about your options for including or excluding the Oracle SYS User in the password profile.

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

Oracle 11g has a default password expiration of 180 days. If an RSA IMG 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 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_ora11_db_scripts.sql for installations using Oracle 11gR2 (11.2.0.3 or 11.2.0.4, 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

Note: This content replaces "About Diagnostic Window Resources" in Chapter 2: "Managing RSA IMG" in the *Administrators Guide*. It includes updated 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 "Configure System Logging Settings" 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.

run-once.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 "Edit Diagnostics Settings" 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 "Generate an RSA IMG Statistics Report" for more information.
- Invalid Database Objects — Lists invalid database objects detected by the system. See "Recompile Invalid Objects" for information on how to re validate the objects.

Migrating Custom Security Contexts

Note: This section replaces the section "Migration from the Pre-6.5 Security Model" in chapter 6 of the *RSA IMG Administrator's Guide V6.9*.

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 IMG 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

Note: In chapter 6 of the *RSA IMG Admistrator's Guide V6.9*, in the topic Adding or Updating Custom Security Contexts, example 2 provides incorrect parameters. The following section replaces 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 JDBC Data Source

Note: This content replaces "Create JDBC Data Sources" in Chapter 2: "Install RSA IMG on WebLogic" in the *Installation on WebLogic Guide V6.9*. It includes information on how to prevent connection to AVPERF errors.

You must create the 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. There are also minor differences in data source configuration between WebLogic versions 10.3.2 and 10.3.4 and greater versions. Review the steps with this information before proceeding.

The following default RSA database user schema names are referenced throughout this section:

- 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 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 your database instance with non-default names, you must use the correct user names and passwords when you create the jdbc data sources.

Create the following JDBC data sources required by RSA IMG:

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

Procedure

1. From the Services menu, select JDBC -> Data Sources (WebLogic 10.3.2 and 10.3.4), or select Data Sources from the menu (WebLogic 10.3.5 and greater).
   Click New to create each data source. From the New button menu for WebLogic 10.3.4 or greater, choose an option:
   - Generic Data Source for a non-Oracle RAC database implementation.
   - Gridlink Data Source for an Oracle RAC database implementation.
2. Configure data sources as follows:
   - 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; Versions 9.01, 9.2.0, 10, 11

Oracle RAC (WebLogic 10.3.2): Oracle's Driver (Thin) for RAC Service-Instance connections; Versions 10, 11.

- 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; Versions 9.01, 9.2.0, 10, 11

    Oracle RAC (WebLogic 10.3.2): Oracle's Driver (Thin) for RAC Service-Instance connections; Versions 10, 11.
  - 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; Versions 9.01, 9.2.0, 10, 11

    Oracle RAC (WebLogic 10.3.2): Oracle's Driver (Thin) for RAC Service-Instance connections; Versions 10, 11.
  - 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; Versions 9.01, 9.2.0, 10, 11

Oracle RAC (WebLogic 10.3.2): Oracle's Driver (Thin XA) for RAC Service-Instance connections; Versions 10, 11.

- Oracle RAC (WebLogic 10.3.4 or greater): 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; Versions 9.01, 9.2.0, 10, 11

    Oracle RAC (WebLogic 10.3.2): Oracle's Driver (Thin XA) for RAC Service-Instance connections; Versions 10, 11.
  - Oracle RAC (WebLogic 10.3.4 or greater): 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

- (WebLogic 10.3.2: Oracle RAC implementation): Select Is this XA Driver
- Database Driver:
  Non-Oracle RAC: Oracle's Driver (Thin XA) for Instance connections; Versions 9.01, 9.2.0, 10, 11

  Oracle RAC (WebLogic 10.3.2): Oracle's Driver (Thin XA) for RAC Service-Instance connections; Versions 10, 11.
- Oracle RAC (WebLogic 10.3.4 or greater): 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
  - (WebLogic 10.3.2: Oracle RAC implementation): Select Is this XA Driver
  - Database Driver:
    Non-Oracle RAC: Oracle's Driver (Thin XA) for Instance connections; Versions 9.01, 9.2.0, 10, 11

    Oracle RAC (WebLogic 10.3.2): Oracle's Driver (Thin XA) for RAC Service-Instance connections; Versions 10, 11.
  - Oracle RAC (WebLogic 10.3.4 or greater): 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.

3. Edit the configuration for each data source:
   - AVDB data source: Connection Pool tab: Set Maximum Capacity to 300.
   - ACMDB, AVDWDB data sources: Connection Pool tab: Set Maximum Capacity to 50.
   - WPDS, WPDS2, WPDS3 data sources: Connection Pool tab: Set Maximum Capacity to 150. (This is the recommended minimum; heavy loads on workflows may necessitate a higher setting.)
4. (Optional) Secure each data source with a security policy. You can elect to enable security after you have successfully installed RSA IMG.
   a. Select the new data source. (AVDB for example) .
   b. Select Security tab > Roles sub-tab
   c. Select New, and then 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.

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.

AFX Ports

AFX Uses the following ports:

- 7777: Used for communication between Mule and MMC8089: Default port for RESTful WebService connectors for receiving asynchronous callback messages. This port will be used by endpoints which process AFX requests asynchronously to send a response back to AFX at a later point in time (once the request has been processed for example). The response would contain information that AFX

can use to determine if the request was successfully processed or if an error was encountered.

- 8444: Configured for installation on WebSphere and WebLogic. See the *Installation on WebSphere Guide V6.9* and the *Installation on WebLogic Guide V6.9* for information on port configuration when AFX is installed those platforms.
- 8585: MMC port
- 61616: ActiveMQ JMS port

Install the AFX Connector Packages

This section describes how to install connector packages for AFX v2.9.x using the RSA IMG application.

Before You Begin

You must download AFX-<version>-Standard-Connectors.zip for this RSA IMG release version from RSA SecureCare Online to a system where you can access RSA IMG application using a web browser.

Procedure

1. Log on to RSA IMG.
2. Select AFX > Import.
3. Browse to the AFX-<version>-Standard-Connectors.zip file.
4. Select Next.
5. Check the Select all items box to select all connector templates listed for import.
6. Select Import to load all standard connector template packages for this released version into the RSA Platform.
7. If you are licensed for one or more AFX Premium Connectors, repeat steps 1 through 5 for AFX-<version>-Premium-Connectors.zip (also located in the packages directory for RSA IMG v6.9.x).

Note: Once the operation completes, connectors and templates in the system that were created from an older version of a package that was imported will be migrated to include enhancements available in the newer version. Those enhancements include new capabilities and settings, fixes for known issues, and any necessary changes to ensure compatibility with AFX server v2.9.x.

Download an AFX Server Archive

For any non-RSA appliance or server, you must download an archive of an AFX server and then install the archive.

Procedure

1. Click the AFX menu and select Servers.
2. From the list of AFX Server configurations, select the server that you want to download.
3. On 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.

4. Specify the download location when prompted by the browser and save the AFX server archive.
5. Install the archive. For more information, see"Install AFX Server Using an Archive Downloaded from RSA IMG" in the *Access Fulfillment Express Guide V2.9*.

Change an AFX Server SSL Certificate

You must change the AFX server's SSL certificate when the certificate has been changed in RSA IMG.

Procedure

1. Click the AFX menu and select Servers.
   The Servers window appears.
2. Select the server for which you want to update the SSL certificate.
   The Server details window appears.
3. Click Change Certificate.
   The Change Certificate window appears.
4. Click OK. RSA IMG generates a new SSL certificate and associates it with the server.
5. Click Download Keystore.
6. Save the client.keystore file to <AFX-home>/mule/conf
7. Restart AFX.

   Note: If you had previously installed this AFX server, until this step is executed, the existing installation with the old server SSL certificate will not be able to communicate with RSA IMG.

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-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-51618	An "ORA-02292 integrity constraint (AVUSER.FK_ CRSUBMISSION_FIELD_ID) violated - child record found" occurs after applying 6.9.0 Patch 2.
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-51644	Weblogic 10.3.6.0 and remote database environment: Migration from 602_HF26_Test_Data to 6.9.0 Patch 2 fails.
ACM-50634	Appendix B of the AFX Guide includes obsolete content. The content will be updated for the next RSA IMG product release.

Tracking ID	Description
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-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-54603	The error message displayed in the log file should be more detailed when RSA IMG cannot be started (acm start) after the avuser password has been changed.