SecurID Governance & Lifecycle Cloud

Release Notes

SecurID
Governance & Lifecycle

Contact Information

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

Trademarks

License agreement

Third-party licenses

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

Note on encryption technologies

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

Distribution

October 2021

Contents

Introduction to SecurID Governance & Lifecycle Cloud

SecurID Governance and Lifecycle Cloud delivers our full-featured, high performing governance solution from the cloud, and provides day-to-day operational support and managed services to free up your internal resources to focus on your core business. Our team of experts let you work smarter by taking responsibility of G&L Solution management tasks using a cloud service for all size enterprises.

The SecurID Governance and Lifecycle Cloud solution lets customers avoid the cost and time of building out their own IT infrastructure to support SecurID G&L and saves operational costs on the maintenance, patching, upgrading and lifecycle management of the solution. The managed services component of the solution reduces the administrative burden on your staff.

What's New in SecurID Governance & Lifecycle Cloud

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

Feature Highlights

Feature	What's New
AFX Retries	AFX Retries can be configured from the AFX user interface and the connector pages when the connection fails between AFX and the AFX connector endpoint. You can configure custom workflows to perform multiple retries by adding loops. A checkbox on the connector settings page lets you override AFX server retry settings. You can also add custom error messages to which the connector retries to match error messages on failure.
SSL Certificates	In Wildfly, SSL certificates for connector and collector endpoints can be managed from a user interface. This eliminates the need to manually add certificates to the keystore files of remote agent and AFX servers.
Pre-migration Utility	The utility creates a patch to generate a summarized ASR-style report and populates new report definitions for a detailed view. These new tabular reports help to re-create local entitlements and manual mappings in a new environment. The report includes: • Applications with local entitlements • Custom files • Manually added/removed account users • Pre and Post custom processing code • Active Data Collectors and Agents list • Entities with ACM managed attributes
Pre/Post custom script processing	Collector creation wizards are enhanced and can define pre and post-processing code. The unification configuration page allows you to specify pre and post-processing code for unification.
Managed attribute migration	This new utility helps when moving managed attributes data to a newer G&L version.
Cloud Supportability	Restart functionality options are provided for the Admin Users to restart the local AFX application and the ACM server nodes from the User interface.
Role Management	In the Commit Changes to Roles page, a limitation is introduced to restrict the number of roles in a single change request. This is to avoid the user from wrongly selecting all the roles that result in a large change request. You can modify the limit from the Role Configuration page.

Additional Feature and Improvement

Feature	What's New
AveksaAdmin Cloud	All SecurID Governance & Lifecycle Cloud super admin users will have unique user names
Migration to Cloud	For existing on-premise users, there is an option to migrate from on-premise to cloud by G&L Cloud solution. All user data is retained and users can quickly continue from where they left.
Trusted Application Support For Web Service	• Client Secret is automatically created and will be displayed for the first time. You can copy the Client Secret for future reference. Based on the business requirements, you can periodically reset the Client Secret by clicking Reset Client Secret icon. The reset action invalidates the existing Client Secret and the application is allowed access using the new Client Secret. • A new field Callback URL is introduced. The security token is returned directly without any redirection when Callback URL is not specified.
REST API ADC Group Membership	With the enhancement of a generic rest account collector for the group membership, the user can map a single group to multiple accounts.
SQL Utility	Support for schema selection along with a specific user authorization option is provided. You can run scripts along with other Data Manipulation Language statements. The Rollback and Commit option is introduced as part of the SQL Utility.
Authentication Sources	• Authentication Source URL - A URL is generated for each authentication source as part of its configuration. This URL is used to make an explicit login using that authentication source. • Explicit ordering - Login logic walks the authentication sources in alphabetical order and picks the first SSO to use from the list. With the enhancement to the feature, the ordering is managed explicitly in the user interface. • Server restart – Any change made to an Authentication Source is reflected immediately and server restart is not required. (Applicable to Wildlfy only)
Granular Scheduling	While creating/editing a collector, review definition, rule, or report, a new option to set up an "Hourly" frequency is seen under the schedule section, if scheduling is enabled. The default intervals are 8 and 12 hours and intervals can be customized.
Reporting and Charting	Bind parameter values can be changed at runtime while running the report. Also, values can be changed from the dashboard as well.

Functional Changes

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

Cloud, Connector

Issue	Description
ACM-112333	If you login in as a G&L Cloud user and the custom setting 'custom.DefaultLocalAgentForAppWizard' is set true, then the local agent (AveksaAgent) is used as a default agent for creating an application using the wizard instead of the remote agent.

CAS Telemetry Uploader

Issue	Description
ACM-109312	All diagnostic data is uploaded to a new RSA-hosted server when sharing is enabled. Ensure the G&L deployment accesses the new server https://telemetry.access.securid.com/.

Fixed Issues

The following issues were fixed in SecurID Governance & Lifecycle Cloud.

Access Request

Issue	Description
ACM-111221	Attribute Synchronizing failed in Active Directory as the initial attribute value was empty. As a fix to the issue, the transformed value is updated from empty value to null.

AFX Server

Issue	Description
ACM-109554	The RACF AFX Connector Reset Password command resets the password successfully, however, the RACF endpoint returns a warning that is interpreted as an error by the AFX command parser. This issue is now fixed and the warning message is now interpreted as a successful password reset message.
ACM-109839	The EDC was collecting both permission set and profiles as entitlements. In the Add Application Role to account capability, only entitlements were added. Profiles are now added to the Add Application Role.

Admin Errors

Issue	Description
ACM-111183	Bulk remove Admin Error. Purging missed for t_exceptions and t_admin_ exceptions_data tables.

API

Issue	Description
ACM-111381	The Generic REST failed whenever the access token expires during a collection. This issue was fixed by adding custom.OauthUseAuthHeaderForClientAuth flag.

ASR

Issue	Description
ACM-111356	ASR generation failed after migration to release 7.2.1 P02. SQL was modified to avoid overflow.

Change Request and Workflow

Issue	Description
ACM-111205	Performance improvement changes were done on the request screen for a better user experience.
ACM-109852	Out of box (OOB) default AFX Manual Fulfillment subprocess was incorrectly configured. Updated the OOB-workflow objects archive which is used in deployment. When the server starts, the updated value for the canceled transitions gets imported into the database.

Issue	Description
ACM-109697	Review CR generation deadlock. As resolution SQL is modified to reduce the chances of the reported deadlocks.

Collector

Issue	Description
ACM-111265	Updates to collector configurations from UI were not saved.
ACM-111149	LDAP group entry “dn” was not assigned to Application Role Custom Attribute during Entitlement Collection.

Custom Attribute

Issue	Description
ACM-111142	G&L system was down after a failed attempt to add user attribute.

Data Collection Processing and Management

Issue	Description
ACM-111567	"Last Successful Collection Date" was not updated for multiple data collectors after re-processing the collector data.

Reviews

Issue	Description
ACM-111240	Changing the due dates in an active review, retriggering all past escalations with a “before the review due date” which had already been completed.

Role Management

Issue	Description
ACM-111396	The instruction field in Role creation did not accept more than 256 characters.
ACM-108594	Parent role was missing the Entitlement tab and was not showing indirect entitlement of child role.

Rules

Issue	Description
ACM-112047	Joiner ruler displays incorrect run message.
ACM-111819	The values present in the value list were getting mapped to a single key hence unauthorized changes were deducted in a rule.
ACM-111387	Attribute Change Rule acted on terminated new users.

Security, ACM Security Model

Issue	Description
ACM-111706	Tomcat Server was upgrade to fix the vulnerability.

Server Core

Issue	Description
ACM-104506	Log Artifacts did not capture rolled over aveksaServer.log files.

UI

Issue	Description
ACM-111411	Unable to delete a business unit, though there were no active users associated with the business unit.
ACM-111058	User's Image inserted through WebServices disappear after restarting the server.

Known Issues and Limitation

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

Tracking ID	Description
Access Certificate ACM-112196	**Issue**: Maintain with expiration for violation remediation review needs a calendar option to customize the date selection.
Access Certificate ACM-112239	**Issue**: "User" and "Rule" links are empty in the User's view for User Access and Violation Reviews.
Access Certificate ACM-112358	**Issue**: In "Data Resource Changes" the "State" section report shows as "Pending Action" for a completed Change Request.
Access Certificate ACM-112238	**Issue**: While performing a rule selection for a Violation Review, the Available rules for selection displays rules which have already been selected, selecting again will create duplicates entries.
Custom Attribute ACM-112382	**Issue**: While adding a custom attribute, the values for decimal type are not given correctly, resulting in a warning popup message. All content edited in the form is reset after the validation.
Docker ACM-112325	The below mentioned warnings "WARN" are seen in the aveksaServer.log/container log during server/container startup only in the container deployment of the product. These warnings do not have an impact on the product's functionality and can be ignored. This is caused due to the mentioned class not being available in the class path during run time. Failed to define class org.apache.cxf.transport.http.policy.HTTPServerAssertionBuilder... Failed to define class org.apache.cxf.transport.http.policy.NoOpPolicyInterceptorProvider... Failed to define class org.apache.cxf.ws.security.policy.WSSecurityPolicyLoader...
Role Management ACM-112236	**Issue**: When creating a "Role Set", the value mentioned in the "Short Description" does not show the value while hovering against the “Role Set” listed in the "Existing Role Set" drop-down list.
Rules ACM-112183	**Issue**: While selecting a new user as a remediator, the user details are blank and include only the title of the user
Rules ACM-112202	**Issue**: Modifying processed rules and rerunning does not work on Test Rule.
Rules ACM-112192	**Issue**: While viewing a Change Request with a Supervisor login, the additional information section is empty and does not show the details passed while generating the Change Request.
Rules ACM-111977	**Issue**: While creating a rule and performing a selection of entitlements for CR creation, all content provided in the form is reset when the Name field has an invalid value.