SecurID Governance and Lifecycle

7.5.2 Patch 07 Release Notes

What's New

The following sections describe the new features and improvements in version 7.5.2 P07.

Cloud

Feature	What's New
ACM-116696	Ability to generate AWR reports from UI for G&L Cloud instances.
ACM-116063	On transition to Cloud, the manually assigned security entitlements must be re-granted manually to each of the users.

Role Management

Feature	What's New
ACM-117627	When a role is maintained at a higher level, both "Role Version Members" and "Definition Tables" are not synchronized with role review.

Functional Changes

Cloud

Feature	What's New
ACM-118474	Removed the option to delete server nodes in UI for cloud instances.

Workflows

Feature	What's New
ACM-116929	Provided an option to select the Remote/Local Agent from the SOAP node in workflow to complete the request by the selected agent. This functionality is added to route the API calls to the selected agent.
ACM-115239	Provided an option to select the Remote/Local Agent from the REST node in a workflow to complete the request by the selected agent. This functionality is added to route the API calls to the selected agent.

Fixed Issues

Access Certification

Issue	Description
SF-02429191 ACM-118277	The custom state button is not displayed in the user access review.
SF-01807741 ACM-111677	No change in status of roles on performing a review result when BRM is off.

Access Request

Issue	Description
SF-02393142 ACM-116676	Partial Rejection of roles still provisions underlying local entitlements.
SF-02378954 ACM-116173	Local Entitlement stays in "Pending Verification" state in the change request in case it is an indirect change item in a role.

Authentication

Issue	Description
SF-02434722 ACM-118563	Active Directory users cannot authenticate to G&L when the "Auto Select" box is not checked in the remote Active directory authentication source.

Collector

Issue	Description
SF-02412127 ACM-117520	REST IDC did not get correct Location attribute data/values in collection result.
SF-02449134 ACM-119297	Failure to map other accounts collected by MAADC, only the first collected account is mapped correctly.
SF-02436443 ACM-118991	"Malformed Fields" error occurs when creating a generic REST account collector.

Change Request and Workflow

Issue	Description
SF-02415086 ACM-117568	Approvals were assigned to the wrong users after the upgrade.
SF-02394063 ACM-117391	When a change request was generated with revocation date, the revoked change request did not resolve the user on account changes.
SF-02366895 ACM-115513	In reviews, change requests were created for the review items removed/deleted outside the review.
SF-02364175, SF-02399003 ACM-115244	Decision Node took the same path for both true and false conditions.
SF-02345231 ACM-114283	User was unable to edit custom escalation workflows, as the "disableEscalationDeleteButton" must be set to “true”.

Email

Issue	Description
SF-02427658 ACM-118316	"Account User Email" column was not shown in the "Account Access and Ownership" display view.

Installer

Issue	Description
ACM-117871	Incorrect version of the package upgradeJDK8u345b01.tar for 7.5.2 P05 on myRSA.

Metadata Import/Export

Issue	Description
SF-02409907 ACM-117865	Import fails (for webservice calls and UI) when user imports a metadata file that contains both active and deleted users as business/technical owners.

Reviews

Issue	Description
SF-02427595 ACM-118231	The custom state button is not displayed in the user access review result.
SF-02404296 ACM-117117	“Sign-off” button used by customerstrings file is fixed to a certain language once there is any modification in the Review name.

Security

Issue	Description
SF-02385438 ACM-117000	An old log4j-1.2.17.jar was not removed from the deployment directory after applying P03 Patch.
SF-02435350 ACM-119042	An old log4j-1.2.17.jar was not removed from the deployment directory after applying P06 Patch.

SSO

Issue	Description
SF-02398228 ACM-117045	When multiple SSO authentication sources are configured, a custom flag (Admin > Settings > Custom), custom.EnableMultipleSSOAuthSource, must be set to “True” to iterate through all the configured SSO one by one until the user is authenticated, otherwise only the first SSO authsource will be picked in order it is set (Admin > System > Authentication).

UI

Issue	Description
SF-02384504 ACM-116382	The System Admin dashboard does not show the IP address.

Known Issues

Issue	Description

ACM-119751,
ACM-119700,
ACM-119770,
ACM-119764,
ACM-119786
	Applying or upgrading to SecurID Governance & Lifecycle (G&L) 7.5.2 P07, where Customer-supplied remote Oracle database is being used, fails with the following error on the UI.
	
	ORA-04063: package body "AVUSER.UTILITIES_PKG" has errors
	
	This does NOT affect GL Cloud, G&L deployments using RSA-provided local/remote database, or G&L deployed on AWS using RDS instances (configured using RSA provided instructions/scripts).
	The error occurs due to a dependency introduced in patch P07 for 7.5.2 that requires certain permissions/grants for the AVUSER schema before applying patch P07 or later.
	
	Resolution
	
	When using a customer-supplied Oracle database, update the AVUSER schema as follows. Note that these steps can be followed PRIOR to applying/upgrading to patch P07, or AFTER you have encountered the error.
	
	1. Login as SYS user (or another user with SYSDBA privilege) in SQLPLUS (or another database tool like SQL Developer) and run the below script to grant Permissions on the below objects to AVUSER.
	
	NOTE: If the schema name is other than the AVUSER, replace the value for v_username with the appropriate SCHEMA name.
	
	`DECLARE`
	`v_username varchar2(100):= 'AVUSER';`
	`BEGIN`
	`-- Create neede grants for 7.5.2P07`
	`EXECUTE IMMEDIATE 'GRANT SELECT ON SYS.DBA_HIST_DATABASE_INSTANCE TO ' || v_username || '';`
	`EXECUTE IMMEDIATE 'GRANT SELECT ON SYS.DBA_HIST_SNAPSHOT TO ' || v_username || '';`
	`EXECUTE IMMEDIATE 'GRANT EXECUTE ON SYS.DBMS_WORKLOAD_REPOSITORY TO ' || v_username || '';`
	`EXECUTE IMMEDIATE 'GRANT EXECUTE ON SYS.DBMS_LOCK TO ' || v_username || '';`

```
-- Recompile the Utilities Package
EXECUTE IMMEDIATE 'ALTER PACKAGE AVUSER.Utilities_Pkg
COMPILE PACKAGE';
EXECUTE IMMEDIATE 'ALTER PACKAGE AVUSER.Utilities_Pkg
COMPILE BODY';
END;
/
```

2. Confirm that the grants were applied, run the following command. The output should list the four grants.

   NOTE: If your SecurID Governance & Lifecycle database schema is configured with a user other than the default AVUSER, please replace 'AVUSER' in the command with the appropriate user.

```
SELECT owner, table_name FROM table_privileges WHERE
grantee = 'AVUSER' and table_name in
('DBA_HIST_DATABASE_INSTANCE',
'DBA_HIST_SNAPSHOT','DBMS_WORKLOAD_REPOSITORY','DBMS_LOCK'
) ORDER BY owner, table_name;
```

3. Confirm that there are no invalid objects in the AVUSER schema. Run the below query.

   NOTE: If your SecurID Governance & Lifecycle database schema is configured with a user other than the default AVUSER, please replace 'AVUSER' in the command with the appropriate user.

```
select * from all_objects where owner='AVUSER' and
status<>'VALID' and object_name ='UTILITIES_PKG';
```

4. Apply the patch P07 again using the original procedure.

Platform Matrix

The latest application server and JDK version have been certified for this release.

	SecurID Governance & Lifecycle Hardware Appliance	SecurID Governance & Lifecycle Software Bundle	Software Only (WebLogic or WebSphere)	Container
Application Server Version				
WildFly 24.0.1 Included	Qualified	Qualified	N/A	Qualified
WebLogic 14.1.1.0	N/A	N/A	Qualified	N/A
WebSphere 9.0.5.15	N/A	N/A	Qualified	N/A
JDK Version Certified				
AdoptOpenJDK 1.8.0_362	Qualified	Qualified	N/A	N/A
Oracle JDK 1.8.0_361 (WebLogic)	N/A	N/A	Qualified	N/A
IBM JDK 1.8.0_361 (WebSphere)	N/A	N/A	Qualified	N/A

Product support with Operating System

Operating System	Customer Supplied Oracle Remote Database	RSA Supplied Local Database	RSA Supplied Database Installed Remotely
SUSE (SLES 12 SP5)	N/A	Qualified	Qualified
Red Hat* (RHEL 8.4, 8.5, 8.6 & 8.7)	N/A	Qualified*	Qualified*

***Installation procedure for Red Hat 8.4+ has additional steps as follows:**

1. **<u>When Installing RSA Supplied Local Database as part of G&L WildFly Installation</u>**

   Before invoking *install.sh*, make changes to *InspectSystem.sh* by following the below steps.

   a. Navigate to the place where deployment files are present:

      (cd /tmp/aveksa/staging/deploy/ENV-setup-scripts).

   b. Edit the InspectSystem.sh (vi InspectSystem.sh).

   c. Remove line no:277 ("bea-stax-api,bea-stax-api,,,").

   d. Save the file.

2. **<u>When Installing RSA Supplied Database on a Remote Host using the Database Tar Package</u>**

   Before invoking *installDatabaseOnly.sh*, make changes to *InspectSystem.sh* by following the below steps.

   a. Navigate to the place where deployment files are present:

      (cd /tmp/aveksa/staging/deploy/ENV-setup-scripts).

   b. Edit the InspectSystem.sh (vi InspectSystem.sh).

   c. Remove line no:277 ("bea-stax-api,bea-stax-api,,,").

   d. Save the file.

Note: If you have a Customer Supplied Oracle Database, no modifications need to be applied to the installation procedure.