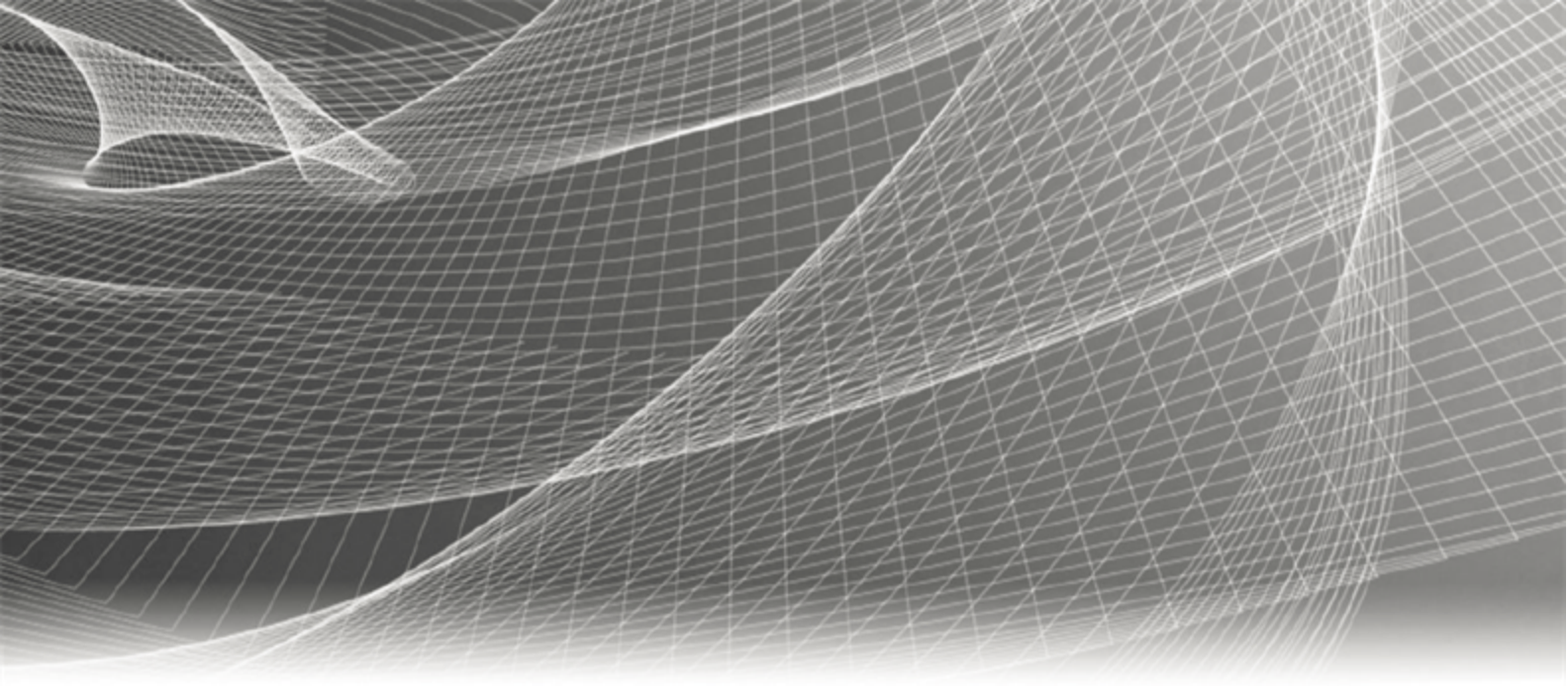

RSA

RSA Identity Governance and Lifecycle

Patch Installation Guide

7.2.1

Contact Information

RSA Community 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 RSA Identity Governance and Lifecycle 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

November 2022

Contents

Installing a Patch

The following procedures describe how to download and apply a patch to RSA Identity Governance and Lifecycle hardware appliance and software bundle installations, and how to upgrade Access Fulfillment Express (AFX) server and connectors. Patches are cumulative.

Important

- When upgrading from product versions older than 7.2.1, you must upgrade to version 7.2.1 before you install any version 7.2.1 patches.
- If you are applying a patch immediately after installing or upgrading, apply the patch in a different shell session from the one in which you ran install.sh.
- Do not attempt to install a previous version of a patch over a later version of a patch.
- When applying a patch in a WebSphere or WebLogic environment, you must uninstall the Workflow Architect EAR before applying updates.

Before you begin

- Customizations made using the RSA Identity Governance and Lifecycle user interface are preserved during the upgrade process. However, any customizations made directly to the EAR are overwritten during the patching process. If you have made any customizations to the EAR, record the customizations before performing the upgrade, and manually restore them after you complete the installation.
- The way in which RSA Identity Governance and Lifecycle handles business descriptions for groups has changed from previous product versions.

  If your RSA Identity Governance and Lifecycle deployment includes business descriptions for groups, run the pre-migration queries for group business descriptions to identify any business descriptions that will be automatically deleted during the update process. For more information and the queries, see Migration Queries for Group Business Descriptions on page 5.
- If your environment uses a customer-supplied database or an RSA-provided database on a remote host, ensure that no database procedures are running against the database schema during the patch installation. The patch process may run SQL against various tables in the database.

  Note: On a deployment with an RSA-provided local database, the patch script automatically stops and starts the database to ensure that this requirement is met.
- In a clustered environment, use only one node during the patch update process. Stop all other nodes in the cluster to ensure that multiple nodes do not attempt a database migration. Before you patch additional nodes or enable farming to push EAR changes to other nodes, validate that the patch is applied and the one node is working as expected.
  For additional details for WebSphere and WebLogic environments, see the *RSA Identity Governance and Lifecycle Installation Guide*. For additional details on WildFly environments, see *RSA Identity Governance and Lifecycle Configuring WildFly Clustering Guide.*

  Note: The created product schemas, such as AVUSER, are reserved for product database objects. Creating additional database objects within the product schemas may affect the operation of the systems, migration, or patch applications.

Migration Queries for Group Business Descriptions

When updating or migrating RSA Identity Governance and Lifecycle from a previous version, RSA Identity Governance and Lifecycle deletes group business descriptions that are not actively in use. Before you migrate, run the following pre-migration queries to identify any group business descriptions that will be deleted by the migration process. If you still need these group business descriptions, you can re-import them with an application reference in the import file, or you can manually recreate them after migration.

Review the results of each query to determine if any of the identified business descriptions are still needed. You must manually recreate or import the identified business descriptions in the new system after migration is complete.

Unused Group Business Descriptions Not Associated with an Application

The following query identifies all group business descriptions that are not associated with an application, and that are currently unused. These business descriptions will be automatically deleted during migration.

```
SELECT
     id,
     'Group' as Type,
     object_filter AS "Object Filter",
     alt_name AS "Display Name",
     short_desc AS "Short Description",
     long_desc AS "Long Description",
     url_ref as "Help Link"
FROM
     t_av_business_description a
WHERE
     NOT EXISTS (
     SELECT
     application_id
FROM
     t_groups b
     WHERE
     b.filter_id = a.id
     )
     AND a.scope_id IS NULL
```

```
    AND a.is_deleted = 'FALSE'
    AND a.object_type = 4
    AND a.applies_to_set = 'FALSE';
```

All Unused Group Business Descriptions

The following query identifies all group business descriptions that are not associated with an application, and that are currently unused. These business descriptions will be automatically deleted during migration.

```
SELECT
    id,
    'Group' as Type,
    object_filter AS "Object Filter",
    alt_name AS "Display Name",
    short_desc AS "Short Description",
    long_desc AS "Long Description",
    url_ref as "Help Link",
    (select name from t_groups where id = a.scope_id) as "Group
    Name",
    (select name from t_applications where id = a.scope_id) as
    "Application Name"
FROM
t_av_business_description a
WHERE
    NOT EXISTS (
    SELECT
    application_id
    FROM
    t_groups b

    WHERE
    b.filter_id = a.id
    )
AND a.scope_id IS NOT NULL
AND a.is_deleted = 'FALSE'
```

```
AND a.object_type = 4
AND a.applies_to_set = 'FALSE';
```

Group Business Description Table

As the ACM schema owner, run the following SQL statement to create a table that allows RSA Identity Governance and Lifecycle to determine a group's business description state during migration.

```
declare
v_tbl_count number;
Begin
     select count(*) into v_tbl_count
     from user_tab_columns
     where table_name = 'TEMP_BUSDESC';
     if v_tbl_count > 0 then
     execute immediate 'drop table temp_busdesc purge';
     end if;
     execute immediate
     'CREATE TABLE temp_busdesc
     AS
          SELECT
          name,
          id,
          filter_id,
          application_id
          FROM
          t_groups
          WHERE
          filter_id !=-1';
end;
/
```

Supported Patch Upgrade Platforms

Follow the steps below to apply the patch on various deployment types:

- WildFly Standalone & Virtual Application
- WildFly Cluster
- WebLogic & WebSphere

Installing the RSA Identity Governance and Lifecycle Patch

Follow these steps to install the RSA Identity Governance and Lifecycle patch:

STEP 1: Download the patch files

1. Log in to RSA Community, and from **Downloads** drop-down list, click **SecurID Governance & Lifecycle**.
2. Click **Full Product Downloads** on the top right of the page.
3. You will be redirected to **myRSA** website after authentication.
4. Select the **Downloads** card, then click RSA Identity Governance and Lifecycle from the list of products.
5. Click the SKU for the product you want to download.
6. From the Select Version drop-down list, select the version/patch you are patching to.
7. Download the following files:
    - Aveksa_<VersionNumber>_P<PatchNumber>.tar.gz
        - For WebSphere: ACM-WebSphere-<VersionNumber>_P<PatchNumber>.tar.gz
        - For WebLogic: ACM-WebLogic-<VersionNumber>_P<PatchNumber>.tar.gz
    - upgradeJDK<version>_<revision>.tar (optional JDK update for security updates)
8. If you have Access Fulfillment Express (AFX), download the following AFX connector packages:
    - AFX-<VersionNumber>_P<PatchNumber>-Standard-Connectors.zip
    - AFX-<VersionNumber>_P<PatchNumber>-Premium-Connectors.zip (SAP customers only)

STEP 2: Shut down all AFX instances

If you have Access Fulfillment Express (AFX) installed, using the AFX user account, shut down all AFX instances before installing the patch upgrade:

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

STEP 3: Install the Patch

In a WildFly Standalone and Virtual Application, do as follows:

1. Copy the patch file Aveksa_<VersionNumber>_P<PatchNumber>.tar.gz to the installation folder (eg: /home/oracle) as root user, and run the following commands to decompress the file:
    i. cd /home/oracle
    ii. tar zvxf Aveksa_<*VersionNumber*>_P<*PatchNumber*>.tar.gz
2. Log in as the user who performed the base installation of RSA Identity Governance and Lifecycle, for example root or the oracle user, as the patch.sh installation script will be run in the directory created in the previous step "**1**".
3. Run the following commands:
    i. cd /home/oracle/Aveksa_<*VersionNumber*>_P<*PatchNumber*>
    ii. sh patch.sh

Note: With each application of a patch, previous versions of the Aveksa EAR are archived in the $AVEKSA_HOME/archive directory. Each archive requires approximately 1 GB of disk space. For more information, see archive/Archive_README.txt.

Note: Applying the patch as root updates the system files created during installation, such as service files and the sudoer file.

To apply a patch on a WildFly Cluster:

Follow the steps in *RSA Identity Governance and Lifecycle Configuring WildFly Clustering Guide*, Chapter 7: "Installing a Patch or Upgrade for RSA Identity Governance and Lifecycle".

To apply a patch in a WebLogic or WebSphere Environment:

1. For detailed instructions, see the section Updating RSA Identity Governance and Lifecycle on WebSphere (or WebLogic) with a Patch in *RSA Identity Governance and Lifecycle Installation Guide*, and the section Upgrade RSA Identity Governance and Lifecycle on WebSphere (or WebLogic) Application Server in *RSA Identity Governance and Lifecycle Upgrade and Migration Guide*.
2. Uncompress and extract the following files from ACM-WebSphere-<VersionNumber>_

P<PatchNumber>.tar.gz or ACM-WebLogic-<VersionNumber>_P<PatchNumber>.tar.gz: aveksa.ear and aveksaWFArchitect.ear

3. Perform any necessary customizations to the Aveksa EAR file. For more information, see "Modifying the RSA Identity Governance and Lifecycle Enterprise Archive" in the *RSA Identity Governance and Lifecycle Installation Guide*.
4. Uninstall the Workflow Architect EAR.
5. Upgrade the Aveksa EAR.
6. Deploy the Workflow Architect EAR.
7. Restart the WebSphere or WebLogic Application Server.
8. In a WebSphere environment, after you deploy the patch, you must restart RSA Identity Governance and Lifecycle. When you start RSA Identity Governance and Lifecycle after applying the patch, SQL processing is performed. After SQL processing is complete, restart RSA Identity Governance and Lifecycle again, to ensure that any patch processing takes effect.
    - To stop and restart RSA Identity Governance and Lifecycle on a WebSphere server:
        i. In the WebSphere console, go to **Applications**.
        ii. Under All Applications, select **aveksa**.
        iii. Click **Stop** to stop the RSA Identity Governance and Lifecycle.
        iv. After the aveksa application has been stopped, click **Start** to start RSA Identity Governance and Lifecycle.
9. In a WebLogic environment, you must restart RSA Identity Governance and Lifecycle after you install the patch.
    - To stop and restart RSA Identity Governance and Lifecycle in a WebLogic environment:
        i. In the WebLogic administrative console, select **Deployments** from the menu.
        ii. Select the Aveksa application and click **Stop** and then **Start** to restart the application.

    Restarting RSA Identity Governance and Lifecycle also restarts the local agent.

STEP 4: Update AFX Server

- If your WildFly deployment includes a local Access Fulfillment Express (AFX), it will be started by the patch script. The AFX server automatically gets upgraded on a startup after the patch is applied.
- If AFX is installed on a remote server (e.g., in WebLogic or WebSphere environment), start AFX server using the AFX user account as follows. The AFX server automatically gets upgraded on a startup after the patch is applied.

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

- If your deployment includes AFX server, you must also upgrade your AFX connectors. For instructions, see Import AFX Connector Packages on page 13.

STEP 5: Update Remote Collection Agents

If your deployment includes a remote Collection Agent, download a new AveksaAgent.zip from RSA Identity Governance and Lifecycle UI. Follow the steps in the *RSA Identity Governance and Lifecycle Upgrade and Migration* Guide to re-install the agent.

Import AFX Connector Packages

If your RSA Identity Governance and Lifecycle deployment uses Access Fulfillment Express (AFX), use this procedure to import the AFX connector package. Reference the instructions in Step 1 above for downloading the connector packages from RSA Community.

Procedure

1. Copy the Connector package files to a directory local to the browser client from which you plan to import the packages:
   - AFX-<*VersionNumber*>_P<*PatchNumber*>-Standard-Connectors.zip
   - AFX-<*VersionNumber*>_P<*PatchNumber*>-Premium-Connectors.zip (SAP customers only)
2. Log on to RSA Identity Governance and Lifecycle.
3. Click **AFX > Import**.
4. Import the packages.
5. Using the AFX user account, start all AFX instances:

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

Upgrade JDK

If the patch includes a new JDK version, follow the steps below to upgrade JDK. This step applies to WildFly and Virtual Application deployments.

1. Stop ACM, AFX, and any remote Collection Agents.
2. Copy the file upgradeJDK<version>_<revision>.tar to the WildFly installation folder, e.g., /home/oracle.
3. Log in as root, and change directory: cd /home/oracle.
4. Decompress the file: tar vxf upgradeJDK<*version*>_<*revision*>.tar.
5. As root user, run the following commands:
   i. cd /home/oracle/upgradeJDK
   ii. chmod -R 744 *
   iii. sh upgradeJDK.sh
6. After JDK is upgraded, log out of all SSH sessions (for root and oracle users). Log back in as needed.
7. Start ACM, AFX, and any remote Collection Agents.