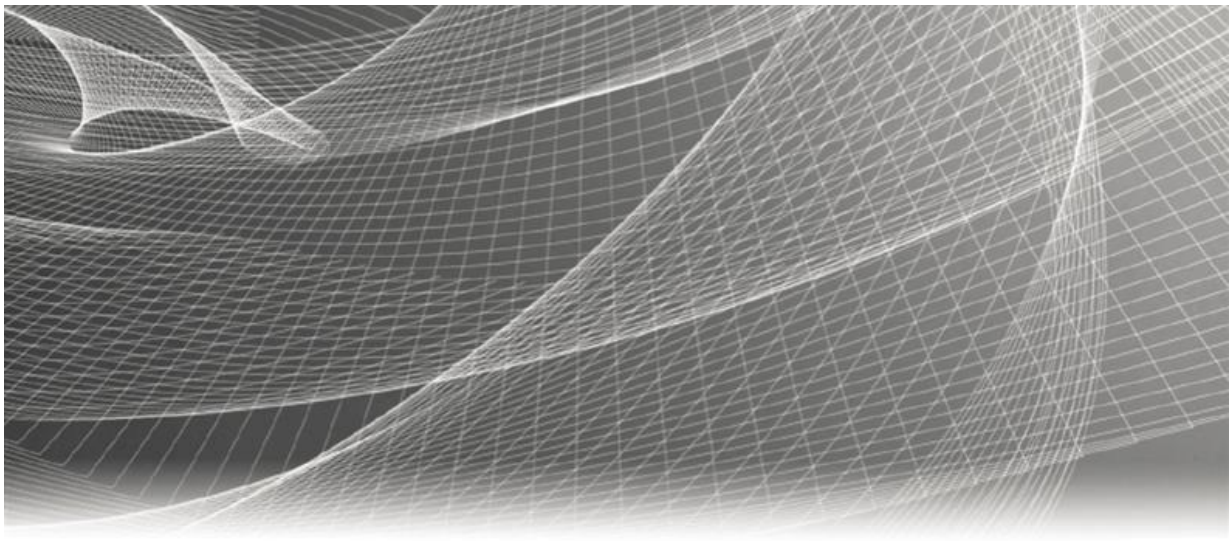


RSA® ARCHER® SUITE

Integration Guide

AWS IAM Access Analyzer - RSA Archer Integration Release 6.7

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers:https://community.rsa.com/community/rsa-customer-support.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and Dell are either registered trademarks or trademarks of Dell Corporation ("Dell") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go towww.emc.com/legal/emc-corporation-trademarks.htm.

License agreement

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

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 on RSA.com. 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.

For secure sites, Dell recommends that the software be installed onto encrypted storage for secure operations.

For customers in high security zones, Dell recommends that a full application sanitization and reinstallation from backup occur when sensitive or classified information is spilled.

Note on Section 508 Compliance

The RSA Archer® Suite is built on web technologies which can be used with assistive technologies, such as screen readers, magnifiers, and contrast tools. While these tools are not yet fully supported, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for RSA Archer.

The RSA Archer Mobile App can be used with assistive technologies built into iOS. While there remain some gaps in support, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for the RSA Archer Mobile App.

Distribution

Use, copying, and distribution of any Dell software described in this publication requires an applicable software license.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice. Use of the software described herein does not ensure compliance with any laws, rules, or regulations, including privacy laws that apply to RSA's customer's businesses. Use of this software should not be a substitute for consultation with professional advisors, including legal advisors. No contractual obligations are formed by publication of these documents.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL INC. 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.

February 2020

Table of Contents

Chapter 1: Overview

About AWS IAM Access Analyzer

AWS IAM Access Analyzer Integration informs which resources in your account that are sharing with external principals as per the configured IAM policies. It does this by using logic-based reasoning to analyze resource-based policies in your AWS environment. An external entity can be another AWS account, a root user, an IAM user or role, a federated user, an AWS service, an anonymous user, or other entity that you can use to create a filter. Access Analyzer generates a finding for each instance of a resource-based policy that grants access to a resource in your zone of trust (your account) to an external entity.

When analyzing the policies, if Access Analyzer identifies one that grants access to an external principal that isn't within zone of trust, it generates a finding. Each finding includes details about the resource, the external entity that has access to it, and the permissions granted so that you can take appropriate action.

Key Features and Benefits

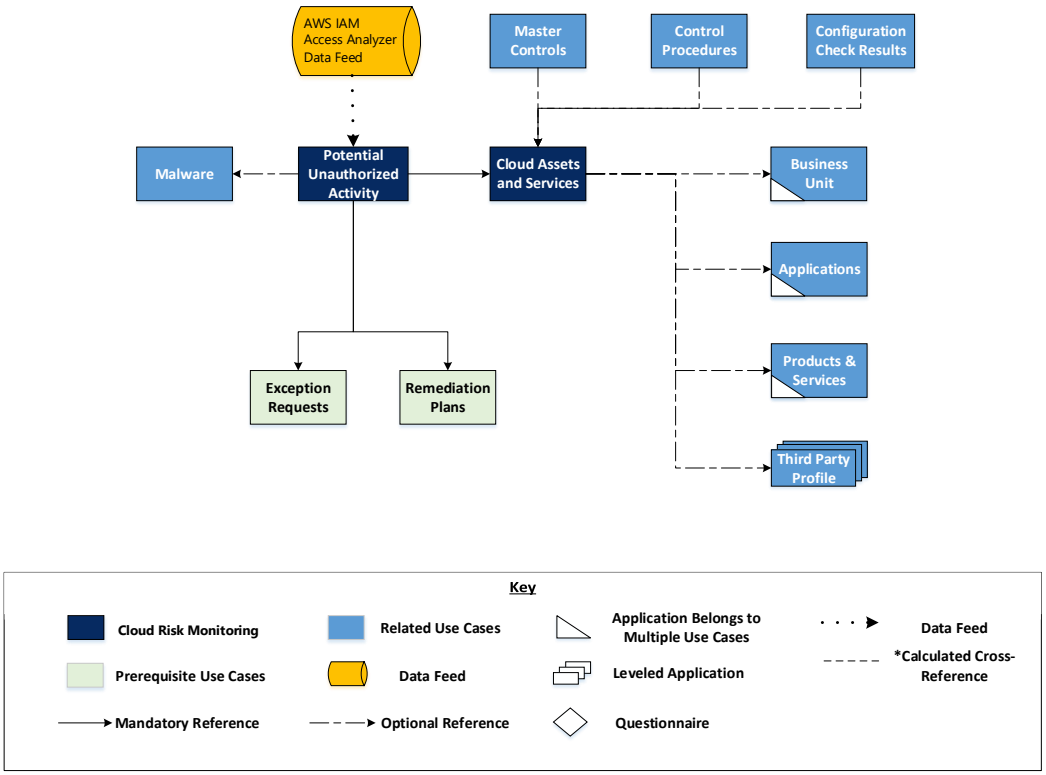
The AWS IAM Access Analyzer Integration with RSA Archer allows you to automatically import finding data directly into on-demand applications for Cloud Risk Monitoring. The integration allows users to view findings linked to the cloud resources. The integration then delivers the tools you need to analyze these findings, automatically notify responsible personnel, and proactively address issues before they impact your organization. Additionally, RSA Archer produces real-time reports and user-specific dashboards to view these findings and their impact to your organization, and to monitor the overall status of your cloud risk monitoring program.

Requirements

Components	Requirement
RSA Archer Solution	RSA Archer IT & Security Risk Management
RSA Archer Use Case(s)	The following use cases can take advantage of the information provided by the AWS IAM Access Analyzer integration: (**Optional**) • RSA Archer IT Risk Management • RSA Archer IT Controls Assurance • RSA Archer IT Security Vulnerability Program • RSA Archer Cyber Incident & Breach Response • RSA Archer Information Security Management System (ISMS) • RSA Archer PCI Management
Requires On-Demand License	Yes. Requires two (2) On-Demand Applications license.
On-Demand Applications	Two On-Demand Applications are required. • Potential Unauthorized Activity • Cloud Assets and Services

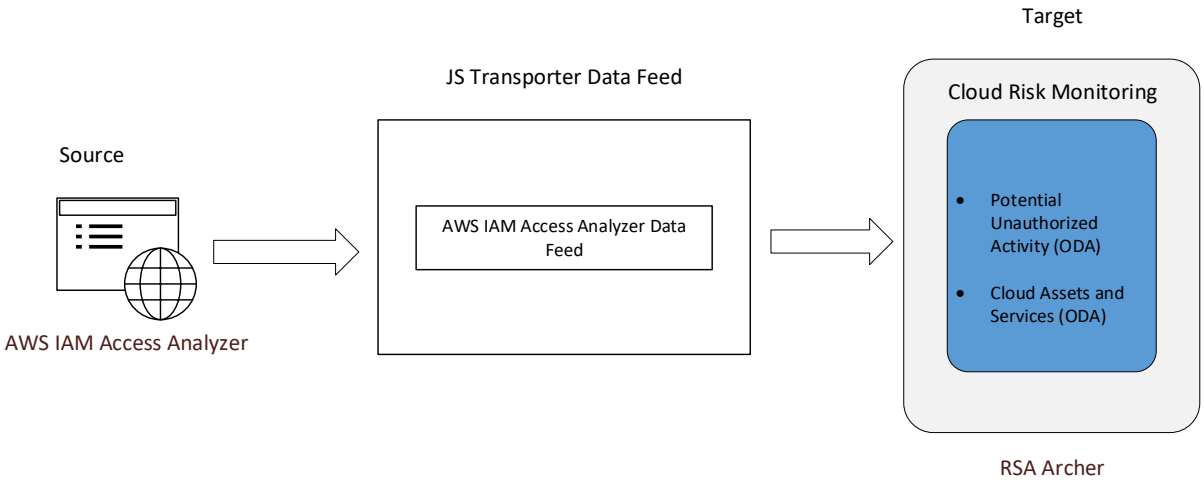
Components	Requirement
Pre-requisite Applications	Requirements for the installation and operation of this integration includes the following applications: • Exception Requests – RSA Archer Issues Management • Remediation Plans – RSA Archer Issues Management
RSA Archer Requirements	RSA Archer release 6.7 or later
AWS IAM Access Analyzer Requirements	Valid AWS IAM Access Analyzer license is required.
Supported Platform Version	This offering has been developed for and validated on RSA Archer Platform release 6.7.

Solution Architecture Diagram



Integration Diagram

The following diagram provides an overview of the interaction between AWS IAM Access Analyzer and RSA Archer.



The integration process follows the following flow:

1. The RSA Archer data feed for the AWS IAM Access Analyzer Integration pulls the findings data from the source: AWS IAM Access Analyzer and imports the data into Target: Potential Unauthorized Activity and Cloud Assets and Services ODA.
2. When the user logins into the AWS IAM Access Analyzer URL, a list of all the findings and a list of resources in your account that you are sharing with external principals available are visible.

Chapter 2: Configure AWS IAM Access Analyzer

Before You Begin

This section provides instructions for configuring the AWS IAM Access Analyzer offering with the RSA Archer Platform. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products to install the required components.

All AWS IAM Access Analyzer endpoint links must be working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Important: The integration described in this guide is being provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.

Access Analyzer analyzes only policies that are applied to resources in the same AWS Region in which it is enabled. To monitor all resources in your AWS environment, you must create an analyzer to enable Access Analyzer in each Region where you're using supported AWS resources.

Obtaining AWS Access Key

Obtain the AWS access keys by contacting the AWS administrator. The access key will be used later in the Data Feed Configuration section.

AWS access keys consist of two parts:

The **access key identifier**. This key can be seen in the IAM console wherever access keys are listed, such as on the user summary page.

The **secret access key**. This is provided when you initially create the access key pair. Just like a password, it cannot be retrieved later. If you lose your secret access key, then you must create a new access key pair.

Enabling Access Analyzer

To enable Access Analyzer in a Region, you must create an analyzer in the Region where you want to monitor access to your resources.

To create an analyzer:

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. Choose Access Analyzer.
3. Choose Create Analyzer.
4. On the Create Analyzer page, confirm that the Region displayed is the Region where you want to enable Access Analyzer.
5. Enter a name for the analyzer.
6. Optional. Add any tags that you want to apply to the analyzer.
7. Choose Create Analyzer.

When you create an analyzer to enable Access Analyzer, a service-linked role named AWSAccessAnalyzerServiceRole is created in your account.

Note: AWS allows you to create only one analyzer per account per Region. Access Analyzer is Regional so it must be enabled in each Region independently.

For more information on AWS Access Analyzer, please follow this link:
https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html

Configure RSA Archer

Before you import the AWS IAM Access Analyzer data feed, complete the following tasks. Install AWS_IAM_Access_Analyzer_RSA_Archer_6.7_Install_Package.zip in your RSA Archer environment, Version 6.7 or above.

Installing the Package

The following tasks detail how to import and install the AWS_IAM_Access_Analyzer_RSA_Archer_6.7_Install_Package.zip.

Task 1: Back up Your Database

There is no Undo function for a package installation. Packaging is a powerful feature that can make significant changes to an instance. It is strongly recommended to back up the instance database before installing a package. This process enables a full restoration if necessary.

An alternate method for undoing a package installation is to create a package of the affected objects in the target instance before installing the new package. This package provides a snapshot of the instance before the new package is installed, which can be used to help undo the changes made by the package installation. New objects created by the package installation must be manually deleted.

Task 2: Import the Package

1. Go to the Install Packages page.
    a. From the menu bar, click .
    b. Under Application Builder, click Install Packages.
2. In the Available Packages section, click Import.
3. Click Add New.
4. Locate and select the package that you want to import.
5. Click OK.
   The package file is displayed in the Available Packages section and is ready for installation.

Task 3: Map Objects in the Package

1. In the Available Packages section, select the package you want to map.
2. In the Actions column, click for that package.
   The analyzer runs and examines the information in the package. The analyzer automatically matches the system IDs of the objects in the package with the objects in the target instances and identifies objects from the package that are successfully mapped to objects in the target instance, objects that are new or exist but are not mapped, and objects that do not exist (the object is in the target but not in the source).

   Note: This process can take several minutes or more, especially if the package is large, and may time out after 60 minutes. This time-out setting temporarily overrides any IIS time-out settings set to less than 60 minutes. When the analyzer is complete, the Advanced Package Mapping page lists the objects in the package file and corresponding objects in the target instance. The objects are divided into tabs, depending on whether they are found within Applications, Solutions, Access Roles, Groups, Sub-forms, or Questionnaires.
3. On each tab of the Advanced Mapping page, review the icons that are displayed next to each object name to determine which objects require you to map them manually.

Icon	Name	Description
	Awaiting Mapping Review	Indicates that the system could not automatically match the object or children of the object to a corresponding object in the target instance. Objects marked with this symbol must be mapped manually through the mapping process. **Important:** New objects should not be mapped. This icon should remain visible. The mapping process can proceed without mapping all the objects. **Note:** You can execute the mapping process without mapping all the objects. The  icon is for informational purposes only.
	Mapping Completed	Indicates that the object and all child objects are mapped to an object in the target instance. Nothing more needs to be done with these objects in Advanced Package Mapping.
	Do Not Map	Indicates that the object does not exist in the target instance or the object was not mapped through the Do Not Map option. These objects will not be mapped through Advanced Package Mapping and must be remedied manually.
	Undo	Indicates that a mapped object can be unmapped. This icon is displayed in the Actions column of a mapped object or object flagged as Do Not Map.

4. For each object that requires remediation, do one of the following:
    - To map each item individually, on the Target column, select the object in the target instance to which you want to map the source object. If an object is new or if you do not want to map an object, select Do Not Map from the drop-down list.

      Important: Ensure that you map all objects to their lowest level. When objects have child or related objects, a drill-down link is provided on the parent object. Child objects must be mapped before parent objects are mapped. For more details, see “Parent and Child Object Mapping” in the RSA Archer Online Documentation.

    - To map all objects in a tab automatically that have different system IDs but the same object name as an object in the target instance, do the following:
        a. In the toolbar, click Auto Map.
        b. Select an option for mapping objects by name:

Option	Description
Ignore case	Select this option to match objects with similar names regardless of the case of the characters in the object names.
Ignore spaces	Select this option to match objects with similar names regardless of whether spaces exist in the object names.

c. Click OK.
The confirmation dialog box opens with the total number of mappings performed. These mappings have not been committed to the database yet and can be modified in the Advanced Package Mapping page.
d. Click OK.

- To set all objects in the tab to Do Not Map, in the toolbar, click Do Not Map.

Note: To undo mapping settings for any individual object, click in the Actions column.

When all objects are mapped, the icon is displayed in the tab title. The icon is displayed next to the object to indicate that the object will not be mapped.

5. Verify that all other objects are mapped correctly.
6. (Optional) To save your mapping settings so that you can resume working later, see "Exporting and Importing Mapping Settings" in the RSA Archer Online Documentation.
7. Once you have reviewed and mapped all objects, click .
8. Select "I understand the implications of performing this operation," and then click OK.
The Advanced Package Mapping process updates the system IDs of the objects in the target instance as defined on the Advanced Package Mapping page. When the mapping is complete, the Import and Install Packages page is displayed.

Important: Advanced Package Mapping modifies the system IDs in the target instance. Any Data Feeds and Web Service APIs that use these objects will need to be updated with the new system IDs.

Task 4: Install the Package

All objects from the source instance are installed in the target instance unless the object cannot be found or is flagged to not be installed in the target instance. A list of conditions that may cause objects not to be installed is provided in the Log Messages section. A log entry is displayed in the Package Installation Log section.

Procedure

1. Go to the Install Packages page.
   a. From the menu bar, click .

b. Under Application Builder, click Install Packages.

2. In the Available Packages section, locate the package file that you want to install, and click Install  .

   Note: Items in the package that do not match an existing item in the target instance are selected by default. All reports will be matched by default. Uncheck the checkbox beside the report to unselect them.
3. In the Selected Components section, select the components of the package that you want to install.
   a. To select all components, select the top-level checkbox.
   b. To install only specific global reports in an already installed application, select the checkbox associated with each report that you want to install.

   Note: Items in the package that do not match an existing item in the target instance are selected by default.
4. Click Lookup.
5. For each component section, do the following:

   Note: To move onto another component section, click Continue or select a component section in the Jump To drop-down menu.
   a. In the Install Method drop-down menu, select an install method for each selected component.

      Note: If you have any existing components that you do not want to modify, select Create New Only. You may have to modify those components after installing the package to use the changes made by the package.
   b. In the Install Option drop-down menu, select an install option for each selected component.

      Note: If you have any custom fields or formatting in a component that you do not want to lose, select Do not Override Layout. You may have to modify the layout after installing the package to use the changes made by the package.
6. Click OK.
7. To deactivate target fields and data-driven events that are not in the package, in the Post-Install Actions section, select the Deactivate target fields and data-driven events that are not in the package checkbox. To rename the deactivated target fields and data-driven events with a user-defined prefix, select the Apply a prefix to all deactivated objects checkbox, and enter a prefix. This can help you identify any fields or data-driven events that you may want to review for cleanup post-install.
8. Click Install.
9. Click OK.

Task 5: Review the Package Installation Log

1. Go to the Install Packages page.
2. Click the Package Installation Log tab.
3. Click the package that you want to view.
4. In the Package Installation Log page, in the Object Details section, click View All Errors.

For a list of packaging installation log messages and remediation information for common messages, see "Package Installation Log Messages" in the RSA Archer Online Documentation.

Configure the Data Feed

AWS IAM Access Analyzer Data Feed is a JavaScript transporter data feed that retrieves data (Findings and Resource-related data) from the AWS IAM Access Analyzer API URL and creates and updates the records in the RSA Archer Potential Unauthorized Activity and Cloud Assets and Services application.

The data feed must be configured. After setting up the data feed, you can schedule them to run **as needed per your organization's requirements**. For more information on Scheduling Data Feeds, see the Scheduling Data Feeds section.

Configure the JavaScript Transporter Settings

Before you upload a JavaScript file, you must configure JavaScript Transporter settings in the RSA Archer Control Panel.

1. On the General tab, go to the **JavaScript Transporter** section.
   a. Open the **RSA Archer Control Panel**.
   b. Go to **Instance Management** and select **All Instances**.
   c. Select the instance you want to use.
   d. On the **General** tab, go to the **JavaScript Transporter** section.
2. In the **Max Memory Limit** field, set the value to 2048 MB (2 GB).
3. In the **Script Timeout** field, set the value to 120 minutes (2 hours).
4. (Optional) If you want to allow only digitally signed JavaScript files in the data feed, enable **Require Signature**.
   a. In the JavaScript Transporter Settings section, select the checkbox **Require Signature**. A new empty cell appears in the **Signing Certificate Thumbprints** section
   b. In the **Signing Certificate Thumbprints** section, double-click an empty cell.
   c. Enter the digital thumbprint of the trusted certificate used to sign the JavaScript file.

      NOTE: For information on how to obtain digital thumbprints, see Obtaining Digital Thumbprints.

      IMPORTANT: If you enable Require Signature and specify no thumbprints, no JavaScript files will be accepted by the system.

   d. (Optional) If you want to add additional thumbprint sources, repeat steps b-c for each thumbprint.
5. On the toolbar, click **Save**.

Obtaining Digital Thumbprints

When running JavaScript data feeds, you can set the RSA Archer instance to only allow digitally signed JavaScript files from trusted sources for security considerations.

For a certificate to be trusted, all the certificates in the chain, including the Root CA Certificate and Intermediate CA certificates, must be trusted on both the Web Server and Services Server machines.

RSA Security LLC cert in the Trusted Root CA Store

RSA Security LLC certificate is not present on every machine's root by default.

1. On the JavaScript file, right-click and select Properties.
   a. Click the Digital Signatures tab.
   b. From the Signature List window, select RSA Security LLC.
   c. Click the Details button.
   d. Click View Certificate.
   e. Click Install Certificate.
   f. Select Local Machine.
   g. Click Next.
   h. Select Place all certificates in the following store and click Browse.
      i. Select Trusted Root Certification Authorities and click OK.
      ii. Click Next.
      iii. Click Finish.
2. Upon successful import, click OK.

Obtaining a Certificate Thumbprint

1. In the RSA Archer Control Panel environment, open the Manage Computer Certificates program.
   a. Click Start.
   b. Type: certificate
   c. From the search results, click **Manage Computer Certificates**.
2. Ensure that your trusted source certificates are in the **Certificates** sub-folder of the **Trust Root Certification Authorities** folder.
3. In the **Certificates** sub-folder, double-click the RSA Security LLC certificate that contains the thumbprint you want to obtain.
4. Verify that the certificate is trusted.
   a. In the Certificate window, click the Certification Path tab.
   b. Ensure that the Certificate Status windows displays the following message:
      THIS certificate is OK
      Note: If the Certificate Status windows displays something different, follow the on-screen instructions.
5. Obtain the trusted certificate thumbprint.
   a. In the Certificate window, click the Details tab.
   b. Select the Thumbprint field.
      The certificate's digital thumbprint appears in the window.
   c. Copy the thumbprint.

Set up the AWS IAM Access Analyzer Data Feeds

Important: Before you upload a JavaScript file, configure JavaScript Transporter settings in the RSA Archer Control Panel. For more information, see Configure the JavaScript Transporter Settings.

1. Go to the **Manage Data Feeds** page.
   a. From the menu bar, click  .
   b. Under Integration, click Data Feeds.
2. Locate and select the: AWS IAM Access Analyzer Data Feed.
   Note: If you are unable to locate the Data Feed. Revisit the package installation section and make sure the data feed component has been included during the installation of the package.
3. Click Open.
4. In the **General Information** section, in the **Status** field, select **Active**.
5. Click the **Transport** tab.
6. In the **Transport Configuration** section, do the following:
   a. Click Upload
   b. From the Upload JavaScript File dialog, click **Add New**.
   c. Locate and select the **AWSIAMAccessAnalyzer.js** file.
   d. Click Open.
   e. From the **Upload JavaScript File** dialog, click **OK**.
7. In the Custom Parameters section, enter key values. The following table describes the value for each key in Custom Parameters.

Key	Value
apiSecret	[Valid value] Default = [empty] (**Required**)
apiCredential	[Valid value] Default = [empty] (**Required**)
region	[Valid value] Default = [empty] (**Required**)
Proxy	[Valid value] Default = [empty] (Optional)

8. The additional parameter shown below provides valid options for the Custom Parameters section for the current JavaScript file.

Key	Value
verifyCerts	[Valid value of true/false] Default = False

9. The additional parameter shown below provides valid **Filter** options for the Custom Parameters section for the current JavaScript file. All the Filter Options are internally using **Contains** operator and are **Case Sensitive**. To filter the data on multiple values, use comma (“,”) as a separator. For Example, to fetch Findings of status “ACTIVE” and “RESOLVED” from AWS Access Analyzer use Filter with “status” as a Key and Value as ACTIVE, RESOLVED. Below are the supported filter types.

Key	Value
resource	[Valid value] Default = [empty] (Optional)
status	[Valid value] Default = [empty] (Optional)
resourceType	[Valid value] Default = [empty] (Optional)
principalAWS	[Valid value] Default = [empty] (Optional)
principalFederated	[Valid value] Default = [empty] (Optional)
principalCanonicalUser	[Valid value] Default = [empty] (Optional)
conditionCognitoIdentity	[Valid value] Default = [empty] (Optional)
conditionGoogleAccount	[Valid value] Default = [empty] (Optional)
conditionPrincipalArn	[Valid value] Default = [empty] (Optional)
conditionPrincipalOrgID	[Valid value] Default = [empty] (Optional)
conditionSourceAccount	[Valid value] Default = [empty] (Optional)
conditionSourceArn	[Valid value] Default = [empty] (Optional)
conditionSourceIp	[Valid value] Default = [empty] (Optional)

conditionSourceVpc	[Valid value] Default = [empty] (Optional)
conditionSourceVpce	[Valid value] Default = [empty] (Optional)
conditionUserId	[Valid value] Default = [empty] (Optional)
conditionFacebookapp_id	[Valid value] Default = [empty] (Optional)
conditionkmsCallerAccount	[Valid value] Default = [empty] (Optional)
conditionEventSourceToken	[Valid value] Default = [empty] (Optional)
conditionS3encryptionid	[Valid value] Default = [empty] (Optional)
conditionAmazonapp_id	[Valid value] Default = [empty] (Optional)
error	[Valid value] Default = [empty] (Optional)

For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log. In the Data Feed Setup window, verify that the key fields are present.

10. Click **Save**.

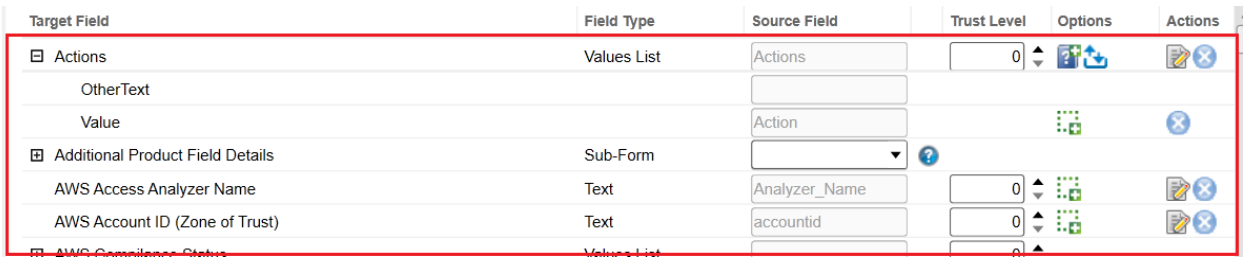
Steps 12, 13, and 14 are optional steps and only needed to troubleshoot or cross verification Field mapping of source and target fields will be pre-configured with the imported data feed. Refer below table for source and target fields mapping.

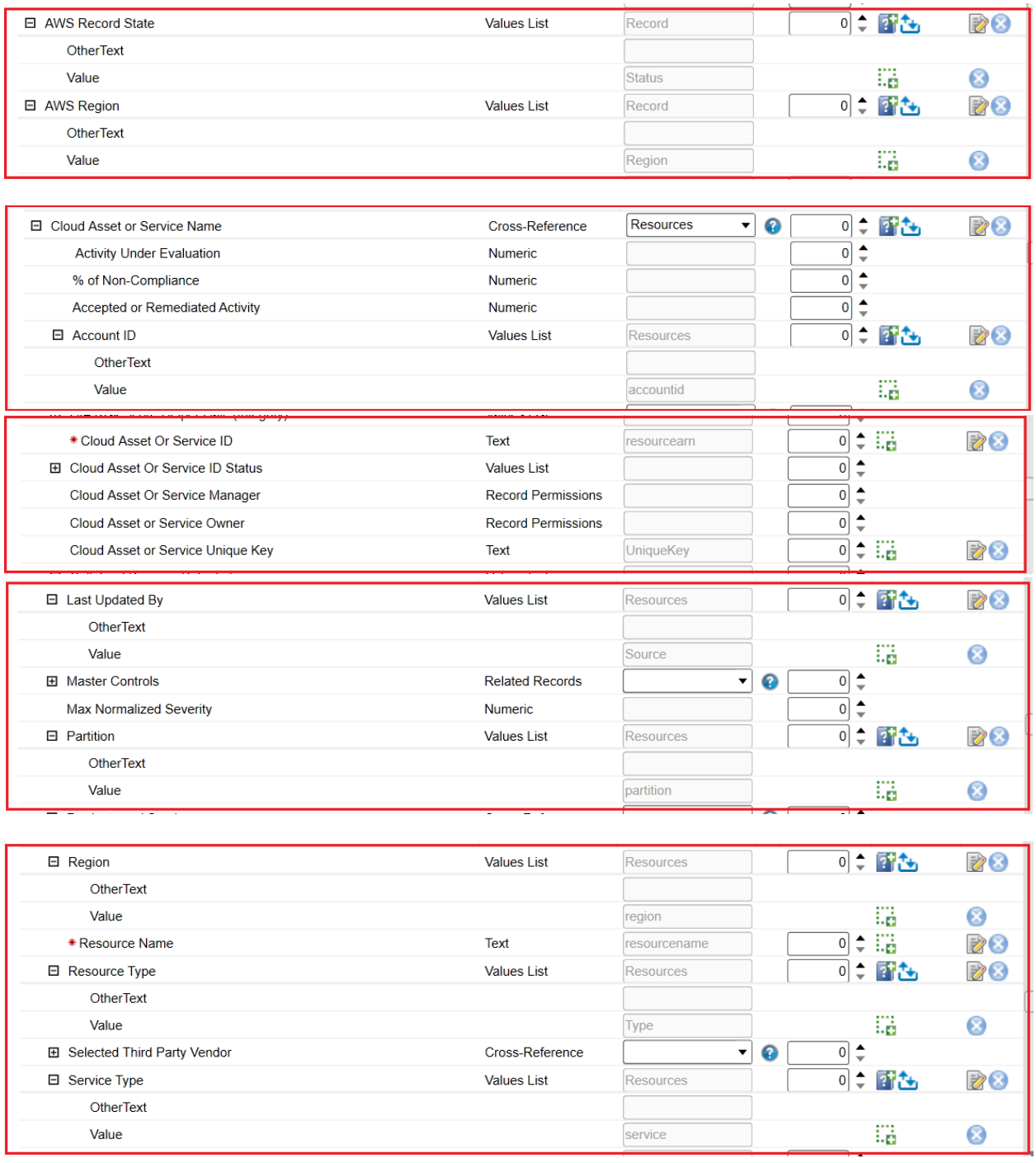
11. Click the **Data Map** tab.
12. In the **Field Map** sub-tab, configure all the source fields (new and modified) to the target Control Standards fields.

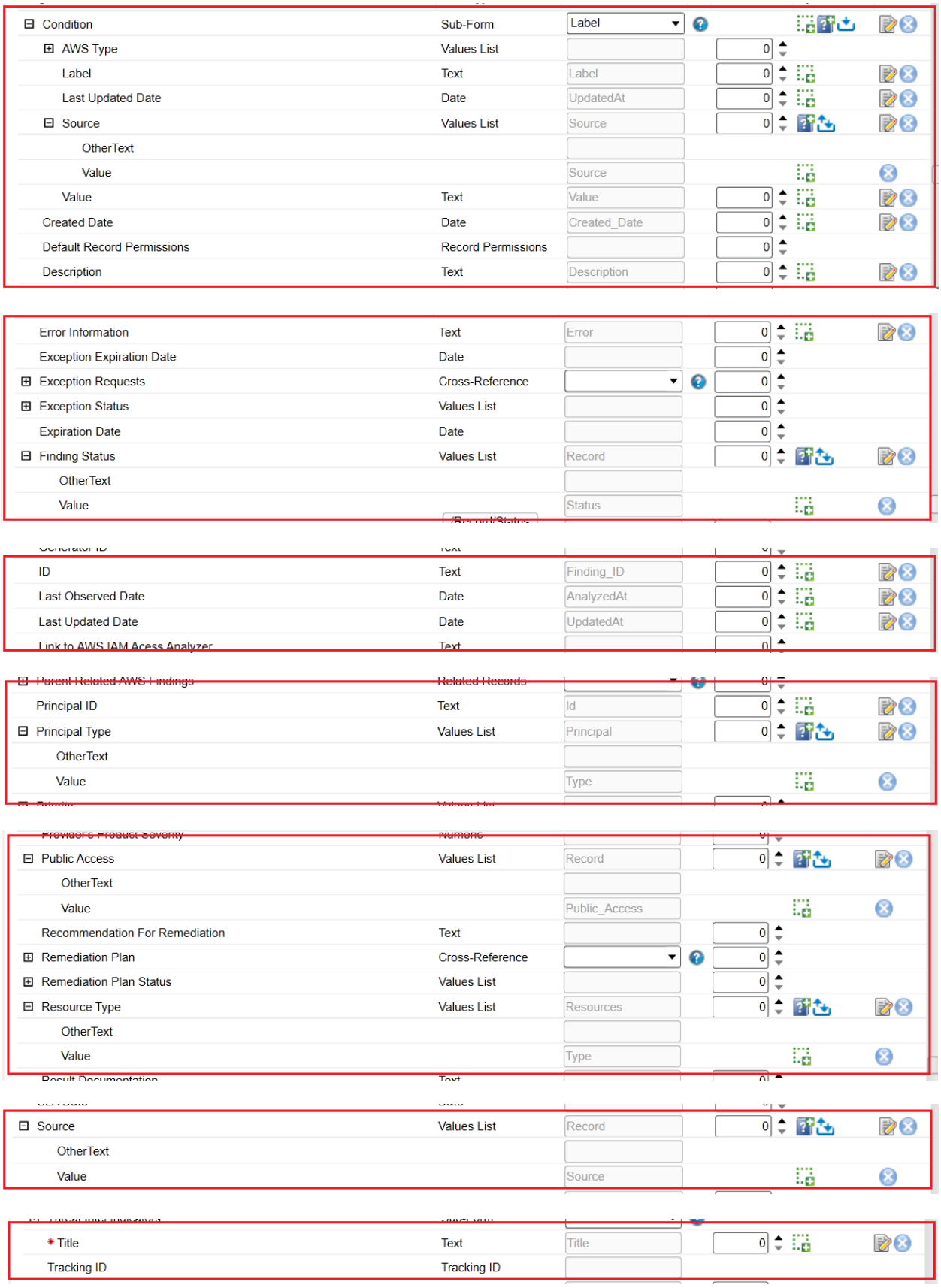
Source Field	Target Field
Actions->Action	Actions
AnalyzedAt	Last Observed Date
Analyzer_Name	AWS Access Analyzer Name
Resource->accountid	AWS Account ID (Zone Of Trust)

Conditions->Condition->Label	Condition: Label
Conditions->Condition->Value	Condition: Value
Source	Condition: Source
UpdatedAt	Condition: Last Updated At
Created_Date	Created Date
Description	Description
Error	Error Information
Finding_ID	ID
Principals->Principal->Id	Principal ID
Principals->Principal->Type	Principal Type
Public_Access	Public Access
Region	Cloud Asset or Service Name: Region
Resources-> accountid	Cloud Asset or Service Name: Account ID
Resources-> partition	Cloud Asset or Service Name: Partition
Resources-> region	Cloud Asset or Service Name: Region
Resources-> resourcearn	Cloud Asset or Service Name: Cloud Asset Or Service ID
Resources-> resourcename	Cloud Asset or Service Name: Resource Name
Resources-> service	Cloud Asset or Service Name: Service Type
Resources-> Source	Cloud Asset or Service Name: Last Updated By
Resources-> Type	Cloud Asset or Service Name: Resource Type
Resources-> UniqueKey	Cloud Asset or Service Name: Cloud Asset Or Service Unique Key
Source	Source
Status	AWS Record State
Title	Title
UpdatedAt	Last Updated Date

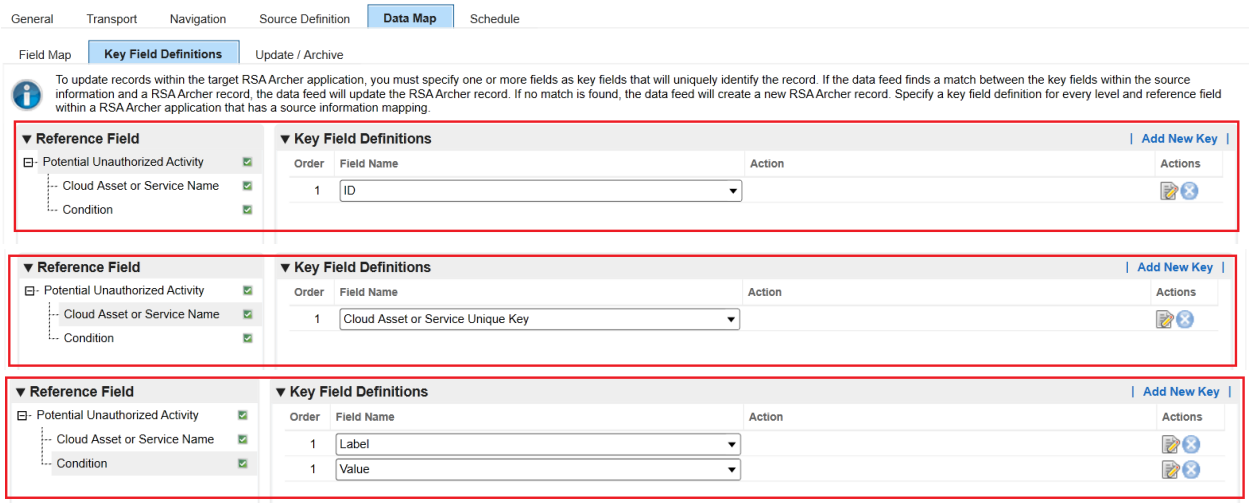
The screen shows below provide examples of these field mappings.







13. In the Key Field Definitions Sub tab, add the “ID” as key field for Control Standards and Sub-Obligations.



Note: AWS IAM Access Analyzer enables per account per region basis. In each region, in the case of IAM roles - findings information is duplicated. If a customer tries to fetch the findings information from all the regions into Cloud Risk Monitoring on-demand applications by using multiple data feeds, roles findings information will be duplicated by default. To avoid the duplicated information, Customer needs to use the filter by Resource types

Scheduling Data Feeds

When you schedule a data feed, the Data Feed Manager validates the information. If any information is invalid, an error message will display. You can save the data feed and correct the errors later, but that data feed is not processed until the errors are rectified.

Important: A data feed must be active and valid to successfully run.

1. Go to the **Schedule** tab of the data feed that you want to modify.
   a. From the menu bar, click .
   b. Under **Integration**, click Data Feeds.
   c. Select the data feed you want to modify.
   d. Click the **Schedule** tab.
2. In the **Recurrences** section, enter the frequency, start and stop times, and time zone for the data feed.
3. *(Optional)* In the Run Data Feed Now section, click Start to override the data feed schedule and run the data feed immediately.
4. Click **Save**.

The following table describes the fields in the **Recurrences** section.

Field	Description
Frequency	Specifies the interval in which the data feed runs. • **By minute:** Runs the data feed by the minute interval set. For example, if you specify 45 in every list, the data feed executes every 45 minutes. • **Hourly:** Runs the data feed by the hourly interval set. For example, every hour (1), every other hour (2), and so forth. • **Daily:** Runs the data feed by the daily internal set. For example, every day (1), every other day (2), and so forth. • **Weekly:** Runs the data feed based on a specified day of the week. For example, every Monday of the first week (1), every other Monday (2), and so forth. • **Monthly:** Runs the data feed based on a specified week of the month. For example, 1st, 2nd, 3rd, 4th, or Last. • **Reference:** Runs a specified data feed as runs before the current one. This option indicates to the Data Feed Service that this data feed starts as soon as the referenced data feed completes successfully. From the Reference Feed list, select after which existing data feed the current data feed starts. A reference data feed will not run when immediately running a data feed. The Data Feed Now option only runs the current data feed.
Every	Specifies the interval of the frequency in which the data feed runs.
Start Time	Specifies the time the data feed begins running.
Start Date	Specifies the date on which the data feed schedule begins.
Time Zone	Specifies the time zone in of the server that runs the data feed.

5. Test the data feed to ensure that all finding details from AWS IAM Access Analyzer were imported into the Potential Unauthorized Activity and Cloud Assets and Services application. If testing fails, try verifying the data feed and rerun. If you experience multiple failures, please contact your RSA Partner.

Appendix A: Certification Environment

Date Tested: Feburary 2020

Product Name	Version Information	Operating System
RSA Archer Suite	Release 6.7 and later	Virtual Appliance
AWS IAM Access Analyzer	NA	NA