Archer® Exchange

Archer® Suite

Version 6.5

Implementation Guide

December 2021

Unified Compliance Framework
Common Controls Hub

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
RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.archerirm.com/company/trademarks. Other trademarks are trademarks of their respective owners.

License Agreement
This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

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 the product documentation page on RSA Link. 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
Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA 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." RSA 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. CUSTOMER IS SOLELY RESPONSIBLE FOR ENSURING THAT THE INSTALLATION OF THE APPLICATION IS PERFORMED IN A SECURE MANNER. RSA RECOMMENDS CUSTOMERS PERFORM A FULL SECURITY EVALUATION PRIOR TO IMPLEMENTATION.

January 2019

Revised: December 2021

Table of Contents

Release Notes

What's New

The following table describes enhancements.

Release Version	Published Date	Notes
Archer 6.5	January 2019	Initial Release
Archer 6.5	December 2021	Re-Signed JavaScript file.

Chapter 1: Overview of UCF Common Controls Hub

Summary

The Unified Compliance Framework (UCF) is an independent initiative to map IT controls across international regulations, standards, and best practices. The UCF harmonizes terms and controls against the backdrop of a master hierarchical list. This allows your organization to focus on a strategic plan (which resources should be applied, when and where) to comply with multiple regulatory bodies using the same team, tools, and funding.

A fundamental starting point is to identify rules, regulations, and industry best practices, which must be included in an organization's compliance portfolio. Parsing the citations within those authoritative sources that contain control objectives and mapping those objectives to organizational controls are the next steps. With those components in place, an organization has a solid foundation to drive audit, risk assessment, asset prioritization, and a host of other activities to support compliance operations.

Integration Features

With the Unified Compliance Framework integration, you will be able to:

- Conveniently overlay organizational control structures with most major authority documents.
- Create composite controls lists by defining simple "acceptance lists" of all relevant controls from selected authorities.
- Clarify conflicts between overlapping authority documents.

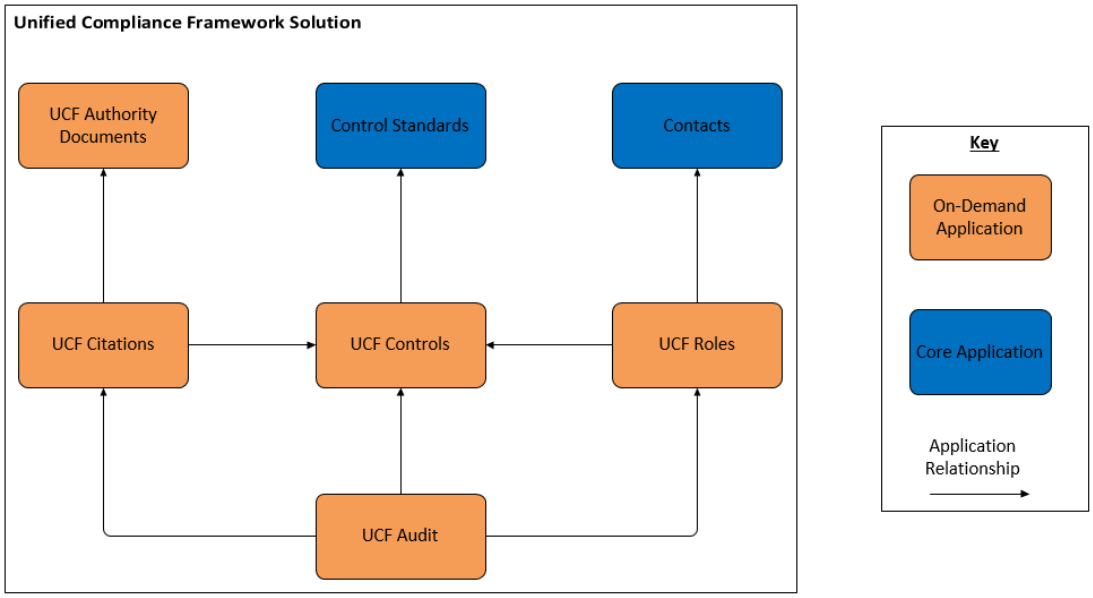
Partner Integration Overview

Components	Prerequisites
Archer Solution Area(s)	Archer Regulatory & Corporate Compliance Management
Archer Use Case(s)	Archer Policy Program Management (Recommended)
Archer Applications	• UCF Audit • UCF Authority Documents • UCF Citations • UCF Controls • UCF Roles
Related Archer Applications	• Control Standards • Contacts
Requires On-Demand License	Yes, 5 (five)

Chapter 2: Integration Components

Integration Diagram

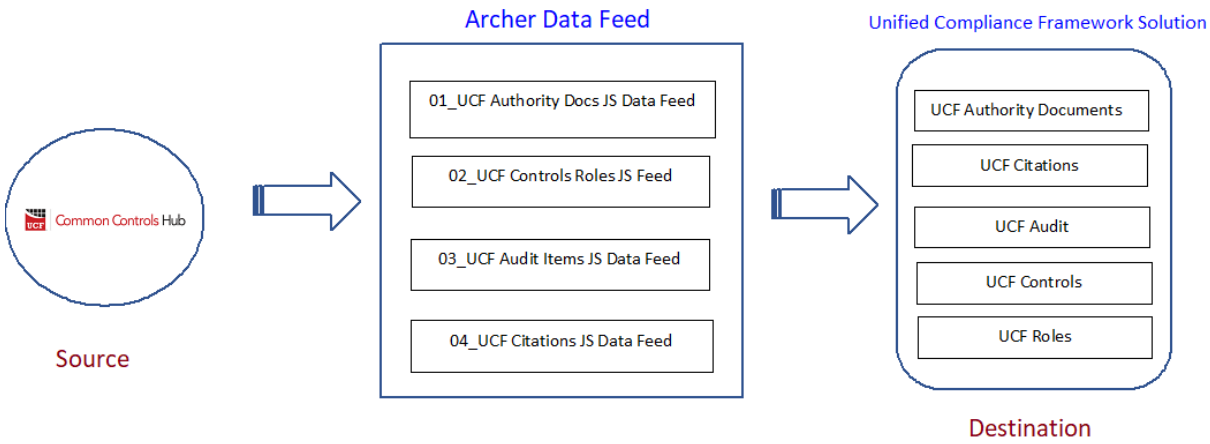
The following diagram provides an overview of interaction of the use cases and application relationships.



Integration Overview

Process Overview

The following diagram provides an overview of interaction between the UCF Common Control Hub website and the Unified Compliance Framework offering.



The integration process follows the following flow:

1. In the UCF Common Control Hub website, the user saves the list ID's, which has the Authority Documents, Citations, Audit Items, Controls and Roles.

2. The RSA Archer data feeds for the Unified Compliance Framework pulls the following data from the source: UCF Common Control Hub website and imports the data into Target: Unified Compliance Framework Solution.
    - UCF Authority Documents
    - UCF Citations
    - UCF Audit Items
    - UCF Controls
    - UCF Roles

Chapter 3: Installation and Configuration

Before You Begin

This section provides instructions for configuring the UCF data feeds for the Unified Compliance Framework offering. 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 must have access to the product documentation for all products in order to install the required components.

The Unified Compliance Framework offering must be installed and 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 provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs of and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.

Prerequisites (System Requirements)

The following applications are required for installation and operation of the UCF Data Feeds for the Unified Compliance Framework offering:

These applications serve as the targets for the data feeds.

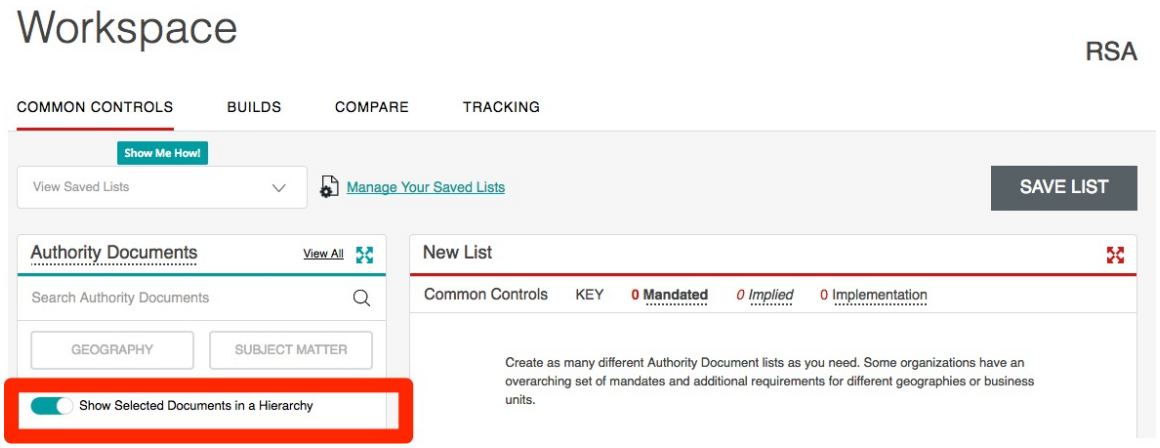
Components	Recommended Software
Archer	Archer release 6.5 or later
Offering Applications	• UCF Audit • UCF Authority Documents • UCF Citations • UCF Controls • UCF Roles
Related Archer Applications	• Control Standards • Contacts
UCF Requirements	Valid UCF license
UCF Patent Information	• U.S. Patent No. 8,661,059 • U.S. Patent No. 9,009,197 • U.S. Patent Application No. 13/952,212 • U.S. Patent Application No. 62/150,237 • U.S. Patent Application No. 13/723,018

UCF Common Controls Hub Configuration

1. Log into the Common Controls Hub (https://cch.commoncontrolshub.com).

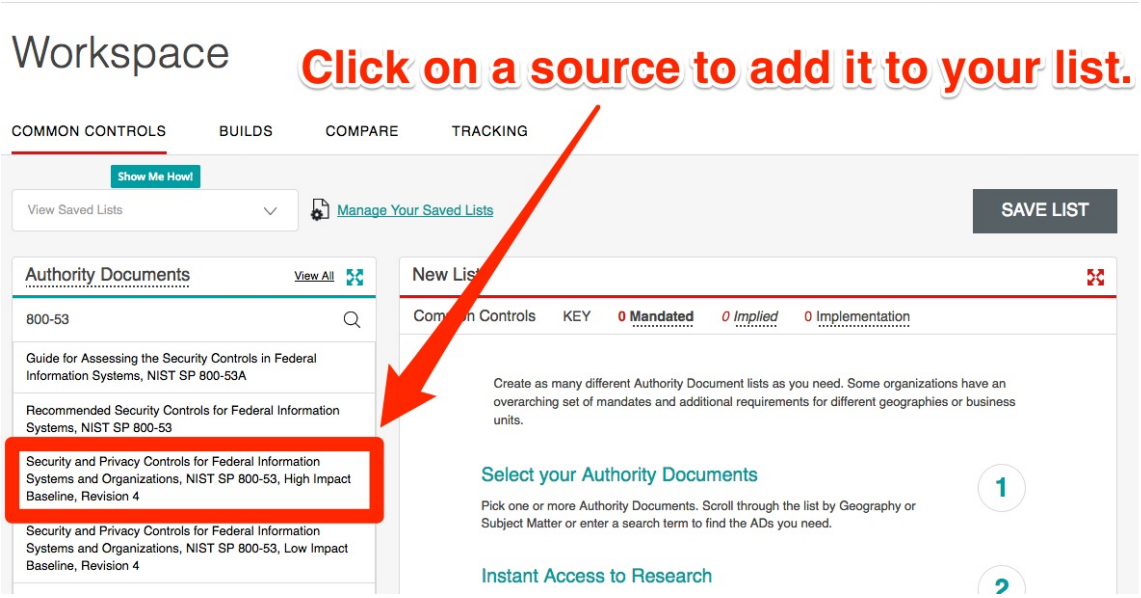
2. Click Workspace.

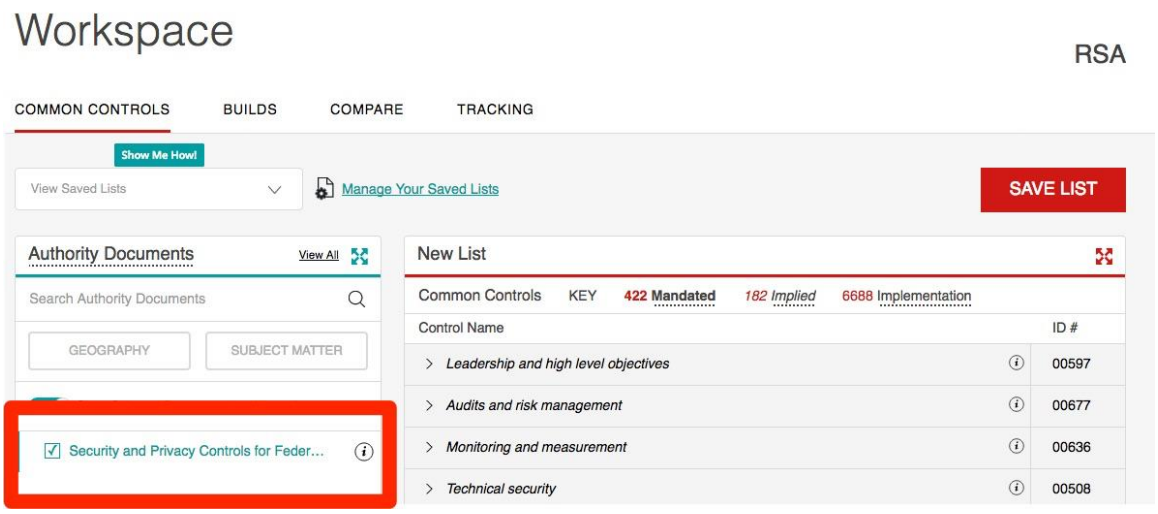
3. Turn on "Show Selected Documents in a Hierarchy."



4. In the Authority Documents section, search for the authority documents that you'd like to move to Archer.

5. Click on the document that you want to add to your list. The documents displays in your list of selected documents.





6. Repeat steps 4 and 5 for each authority document that you want added to Archer.

7. Click “Save List.”

8. Name your list and enable “**Share this List**” check box. You will use this name later in generating the UCF content for Archer.

Create API key In UCF Common Controls Hub:

This API key is used to configure the solution in “Data Feed Configuration”. Refer to the UCF documentation on https://support.commoncontrolshub.com/.

Data Feed Configuration

The following data feeds are used as part of the UCF integration process:

- **01_UCF_Authority_Docs_JS_Data_Feed** is a JavaScript transporter data feed that fetches data from https://api.unifiedcompliance.com/cch-ad-list/<list>/authority-documents and creates and updates the records in the UFC Authority Documents application.

- **02_UCF_Controls_Roles_JS_Feed** is a JavaScript transporter data feed that fetches data from https://api.unifiedcompliance.com/cch-ad-list/<list>/tracked-controls/details and creates and updates the records in the UCF Controls and UCF Roles application.

- **03_UCF_Audit_Items_JS_Data_Feed** is a JavaScript transporter data feed that fetches implicit and explicit audit data**.**
  Explicit data: [https://cch.commoncontrolshub.com/] https://api.unifiedcompliance.com/cch-ad-list/<list>/audit-items
  Implicit data: https://api.unifiedcompliance.com/audit-item/<audit_id>/details creates and updates the records in the UCF Audit application.

- **04_UCF_Citations_JS_Data_Feed** is a JavaScript transporter data feed that fetches data from https://api.unifiedcompliance.com/authority-document/ID/citations and creates and updates the records in the Citations application.

There are four data feeds available for the Unified Compliance Framework solution. All data feeds must be configured.

Import and run the data feeds in the following order:

1. Set up the **01_UCF_Authority_Docs_JS_Data_Feed**
2. Set up the **02_UCF_Controls_Roles_JS_Feed**
3. Set up the **03_UCF_Audit_Items_JS_Data_Feed**
4. Set up the **04_UCF_Citations_JS_Data_Feed**

After setting up the data feed, you must configure the data feed. You can schedule data feeds to run as needed per the requirements for your organization. For more information on Scheduling Data Feeds, see Scheduling Data Feeds.

Configure the JavaScript Transporter Settings

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

1. On the general tab, go to the JavaScript Transporter section.
    a. Open the 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) To allow only digitally signed JavaScript files in the data feed, enable the Require Signature option.
    a. In the JavaScript Transporter Settings section, select the Require Signature checkbox. 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 tollbar, click Save.

Obtaining Digital Thumbprints

When running JavaScript data feeds, you can set the system 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.

Archer Technologies LLC Cert in the Trusted Root CA Store

Archer Technologies LLC certificate is not present on every machine's root by default.

1. On the JavaScript file, right-click and select Properties.
2. Click the Digital Signatures tab.
3. From the Signature List window, select Archer Technologies LLC.
4. Click the Details button.
5. Click View Certificate.
6. Click Install Certificate.
7. Select Local Machine.
8. Click Next.
9. Select Place all certificates in the following store and click Browse.
    a. Select Trusted Root Certification Authorities and click OK.
    b. Click Next.
    c. Click Finish.
10. Upon successful import, click OK.

Obtain a Certificate Thumbprint

1. In the 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 Archer Technologies 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:
    c. 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 UCF Authority Documents Feed

Important: Before you upload a JavaScript file, configure JavaScript Transporter settings in the 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. In the Manage Data Feeds section, click Import.
3. Locate and select the **01_UCF_Authority_Docs_JS_Data_Feed.dfx5** file for the data feed.
4. Click Open.
5. In the General Information section, in the Status field, select Active.
6. Click the **Transport** tab.
7. In the **Transport Configuration** section:
    a. Click **Upload**.
    b. From the **Upload JavaScript File** dialog, click Add New.
    c. Locate and select the **ucf_api_complete.js** file
    d. Click **Open**.
    e. From the Upload JavaScript File dialog, click **OK**.
8. In the Custom Parameters section, enter key values.
   The following table describes the value for each key in Custom Parameters.

Key	Value
apikey	*[Valid value]*
listName	*[Valid value]*
adurl	https://api.unifiedcompliance.com/cch-ad-list/<list>/authority-documents
dataSource	adocs

Note: The listed values are in place by default. They can be configured to suit your environment.

9. 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.
10. Verify that key field values are not missing from the data feed setup window.
11. Click **Save**.

Set Up the UCF Controls and Roles Feed

Before you upload a JavaScript file, you must 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. In the Manage Data Feeds section, click Import.
3. Locate and select the **02_UCF_Controls_Roles_JS_Feed.dfx5** file for the data feed.
4. Click Open.
5. In the General Information section, in the Status field, select **Active**.
6. Click the Transport tab.
7. In the Transport Configuration section, complete the following:
    a. Click **Upload**.
    b. From the Upload JavaScript File dialog, click Add New.
    Locate and select the **ucf_api_complete.js** file and click Open.
    c. From the Upload JavaScript File dialog, click **OK**.
8. In the Custom Parameters section, enter key values.
9. The following table describes the value to enter for each key in Custom Parameters.

Key	Value
apikey	*[Valid value]*
listName	*[Valid value]*
adurl	https://api.unifiedcompliance.com/cch-ad-list/<list>/authority-documents
trcurl	https://api.unifiedcompliance.com/cch-ad-list/<list>/tracked-controls/details
dataSource	Control

Note: The listed values are in place by default. They can be configured to suit your environment.

10. 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.
11. Verify that key field values are not missing from the data feed setup window.
12. Click **Save**.

Set Up the UCF Audit Data Feed

Before you upload a JavaScript file, you must 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. In the Manage Data Feeds section, click Import.
3. Locate and select the **03_UCF_Audit_Items_JS_Data_Feed.dfx5** file for the data feed.
4. Click Open.
5. In the General Information section, in the Status field, select **Active**.
6. Click the Transport tab.
7. In the Transport Configuration section, complete the following:
    a. Click **Upload**.
    b. From the Upload JavaScript File dialog, click Add New.
    c. Locate and select the **ucf_api_complete.js** file and click Open.
    d. From the Upload JavaScript File dialog, click **OK**.
8. In the Custom Parameters section, enter key values.

The following table describes the values to enter for each key in Custom Parameters.

Key	Value
apikey	*[Valid value]*
listName	*[Valid value]*
adurl	https://api.unifiedcompliance.com/cch-ad-list/<list>/authority-documents
expauditurl	https://api.unifiedcompliance.com/cch-ad-list/<list>/audit-items
dataSource	auditItems
explicitAuditItems	Yes - If Explicit No - If Implicit

Note:

- The listed values are in place by default. They can be configured to suit your environment.
- 'explicitAuditItems' key default value is set with Yes, it uses UCF attestation API to fetch the audit items.

9. 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.
10. Verify that key field values are not missing from the data feed setup window.
11. Click **Save**.

Set Up the UCF Citations Data Feed

Before you upload a JavaScript file, you must 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. In the Manage Data Feeds section, click Import.
3. Locate and select the **04_UCF Citations JS Data Feed.dfx5** file for the data feed.
4. Click Open.
5. In the General Information section, in the Status field, select **Active**.
6. Click the Transport tab.
7. In the Transport Configuration section, complete the following:
    a. Click **Upload**.
    b. From the Upload JavaScript File dialog, click Add New.
    c. Locate and select the **ucf_api_complete.js** file and click Open.
    d. From the Upload JavaScript File dialog, click **OK**.
8. In the Custom Parameters section, enter key values.

The following table describes the values to enter for each key in Custom Parameters.

Key	Value
apikey	*[Valid value]*
listName	*[Valid value]*
adurl	https://api.unifiedcompliance.com/cch-ad-list/<list>/authority-documents
dataSource	citations

Note: The listed values are in place by default. They can be configured to suit your environment.

9. 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.
10. Click the Source Definition tab.
    a. Click the Tokens sub-tab.
    b. Verify token values.

    The following table describes token values to verify.

Token	Value
LastRunTime	(Populated by Data feed)
CrossReferencesMode	LinkOnly
RelatedReferencesMode	LinkOnly
BatchContentSave	1000

Note: For more information about tokens, see **Data Feed Tokens** in the **Archer Online Documentation**.

11. Verify that key field values are not missing from the data feed setup window.
12. Click **Save**.

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 the 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. Complete the Recurrences section.
   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.

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.

Chapter 4: Installing Archer Unified Compliance Framework

Complete the following tasks to install the offering.

Step 1: Prepare for the Installation

1. Ensure that your Archer system meets the following requirements:
    - Archer Platform version 6.5
2. Download the ODA install package from the Archer Exchange on RSA Link: https://community.rsa.com/t5/archer-exchange/ct-p/archer-exchange
3. Read and understand the "Packaging Data" section of the Archer Online Documentation.

Step 2: Install the Package

Installing a package requires that you import the package file, map the objects in the package to objects in the target instance, and then install the package. See Installing the Application Package for complete information.

Step 3: Set up Data Feeds

Import and test the following data feeds:

- 01_UCF_Authority_Docs_JS_Data_Feed
- 02_UCF_Controls_Roles_JS_Feed
- 03_UCF_Audit_Items_JS_Data_Feed
- 04_UCF_Citations_JS_Data_Feed

Step 4: Test the Installation

Test the Archer Unified Compliance Framework according to your company standards and procedures, to ensure that the use case works with your existing processes.

Installing the Package

The following steps detail how to import and install the application package

Step 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. RSA strongly recommends backing 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.

Step 2: Import the Package

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, click Import.
3. Click Add New, then locate and select the package file that you want to import.
4. Click OK.
   The package file is displayed in the Available Packages section and is ready for installation.

Step 3: Map Objects in the Package

Procedure

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 "Mapping Parent/Child Objects" in the RSA Archer Online Documentation.
    - To automatically map all objects in a tab 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 the 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 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.

Step 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.
3. In the Configuration section, select the components of the package that you want to install.
    - To select all components, select the top-level checkbox.
    - 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. In the Configuration section, under Install Method, select an option for each selected component. To use the same Install Method for all selected components, select a method from the top-level drop-down list.

    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.
5. In the Configuration section, under Install Option, select an option for each selected component. To use the same Install Option for all selected components, select an option from the top-level drop-down list.

    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. 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.
7. Click Install.
8. Click OK.

Step 5: Review the Package Installation Log

1. Go to the Package Installation Log tab of the Install Packages page.
    a. From the menu bar, click  .
    b. Under Application Builder, click Install Packages.
    c. Click the Package Installation Log tab.
2. Click the package that you want to view.
3. In the Package Installation Log page, in the Object Details section, click View All Warnings.

Appendix A: Certification Environment

Date Tested: January 2019

Product Name	Version Information	Operating System
Archer	6.5 and later	Virtual Appliance
UCF CCH	NA	NA