# RSA® ARCHER® SUITE
# Integration Guide

KONEXUS - RSA Archer Integration Release 6.5

## 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.


August 2019

# Table of Contents

# Chapter 1: Overview

## About RSA Archer – KONEXUS Integration

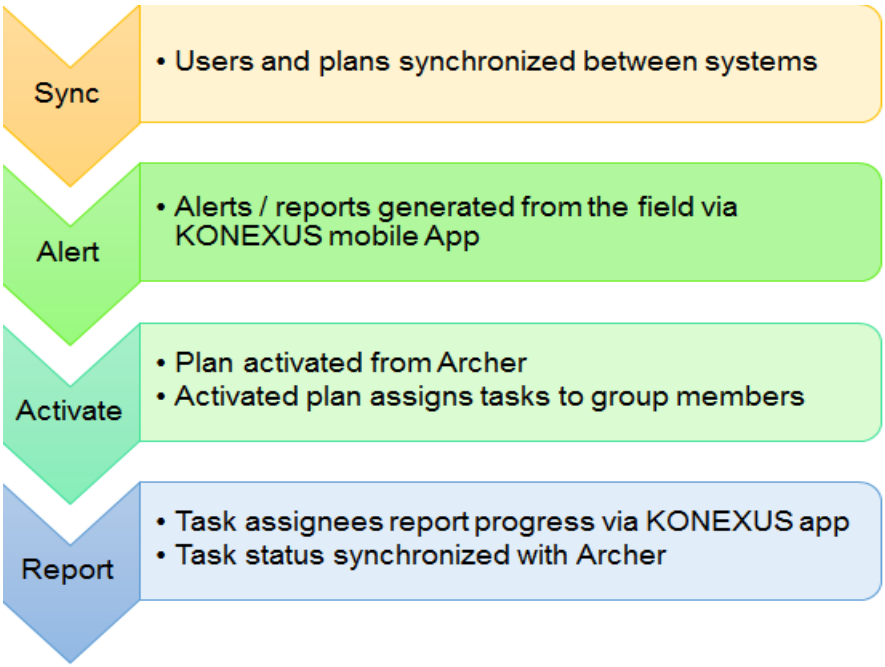
The RSA Archer - KONEXUS integration for iPhone and Android synchronizes with the RSA Archer Business Continuity BC/DR plans, enabling users to view business continuity or disaster recovery plans and associated strategies, tasks, call trees, and requirements from their Apple iOS and Android devices. The mobile application supplements hard copy plans when a user may not have access to their RSA Archer instance during a crisis. If the data center goes down during a disaster or crisis, the end user will still have access to plans, ready to act.

The integration streamlines crisis response and transforms RSA Archer business continuity and crisis management plans into actionable, role-based, task lists that put critical information in the hands of users via their mobile devices.

Task lists can be created in KONEXUS based on an Activated Plan in Archer. This delivers instantly to the designated teams for completion on a mobile app, giving better visibility into the progress of task lists. Recovery Coordinators can monitor completion of task lists and recovery status from the mobile app or Archer. Crisis Incidents created in Archer are published to mobile users for selection in Crisis/Incident Reporting.

The use cases addressed in the integration:

- Send Alert from KONEXUS Mobile → Crisis Manager
- Crisis Manager Activates a crisis in Archer
- Connector Service creates crisis in KONEXUS system
- Connector Service sends Archer Task to KONEXUS system
- Connector Service receives task updates from KONEXUS system and updates the Archer tasks
- Connector Service copies BCDR Plan from Archer to KONEXUS



## Key Features and Benefits

With the RSA Archer - KONEXUS Integration, you can:

- Provide mobile access to the plans and critical content (even if RSA Archer or the network is unavailable).
- Deliver actionable task lists to mobile teams, with real-time monitoring of completion/recovery status.
- Simplify crisis or incident reporting from the scene, with situational intelligence delivered through automated escalation paths based on event type and role.
- Enhance collaboration with global, multilingual teams with in-stream translation of secure chat conversations, alerts, polls, and tasks.
- Enable monitoring of risks, and assessment and response to reported events.
- Alert site users and mobile travelers in selected areas to quickly account for safety and status.
- Accelerate your response to crisis events by providing responders immediate access to recovery plans
- Reduce negative impacts on revenue, brand image, and stakeholder confidence because of accelerated response.

## Requirements

| Components | Requirement |
|---|---|
| **RSA Archer Solution** | • RSA Archer Business Resiliency |
| **RSA Archer Use Case(s)** | • RSA Archer Business Continuity and IT Disaster Recovery Planning<br>• RSA Archer Crisis Management |
| **RSA Archer Applications** | • BC/DR plans<br>• Recovery Strategies<br>• Recovery Tasks<br>• Roles and Responsibilities<br>• Activated Plans<br>• Testing/Exercise<br>• Crisis Events |
| **Uses Custom Application** | No |
| **Requires On-Demand License** | No |
| **RSA Archer Requirements** | RSA Archer release 6.5 or later |
| **KONEXUS Requirements** | Valid KONEXUS license is required |

## KONEXUS Integration Service Prerequisites

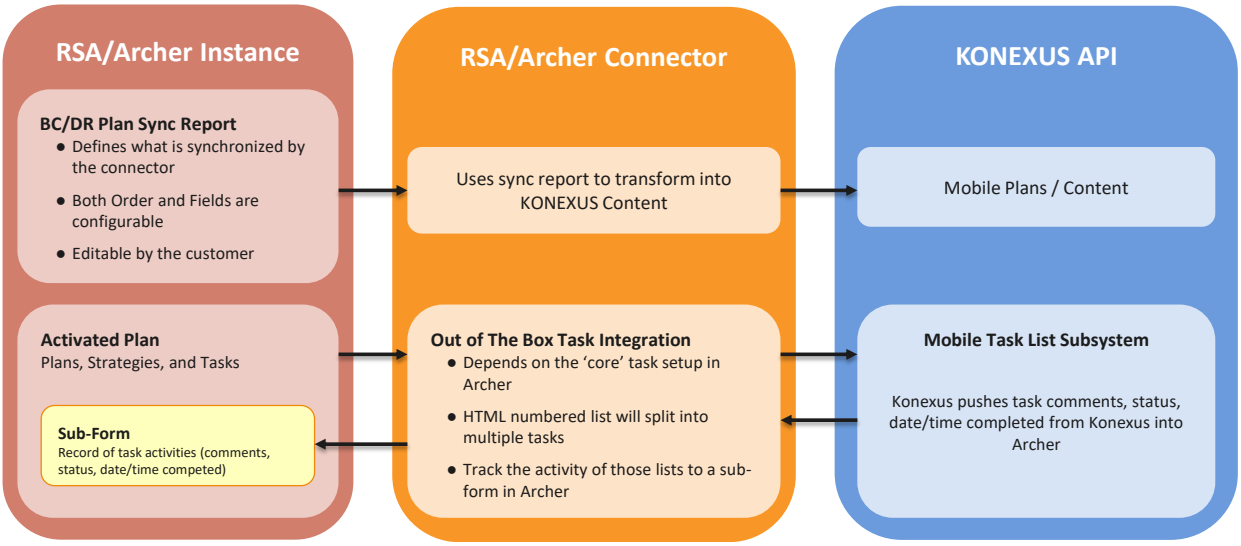
| Components | Recommended Software |
|---|---|
| **Operating System** | Windows Server 2012 R2 and above |
| **Web Server** | Microsoft Internet Information Services<br>(Included in Windows Server 2012 R2 or 2016) |
| **Framework** | Microsoft .Net framework 4.5.2 and above |
| **Deployment Requirements** | Connector service can be deployed on the same server or on a different server that is hosting the RSA Archer Platform.<br><br>It is recommended to deploy the Connector service on a different server with the above recommended software.<br><br>Connector REST Endpoint component should be deployed on a public IP host so KONEXUS who is outside the network can communicate. |
| **Network Requirements** | The KONEXUS Connector Service and REST Endpoint component should have network access to RSA Archer. The REST Endpoint component should be running on a Public IP and port must be opened to accept the inbound traffic. |
| **App Device Requirements** | Android/iOS |
| **Supported Platform Version** | This offering has been developed for and validated on RSA Archer Platform release 6.5. |
| **Pre-requisite RSA Archer use cases** | • RSA Archer Business Continuity and IT Disaster Recovery Planning<br>• RSA Archer Crisis Management |

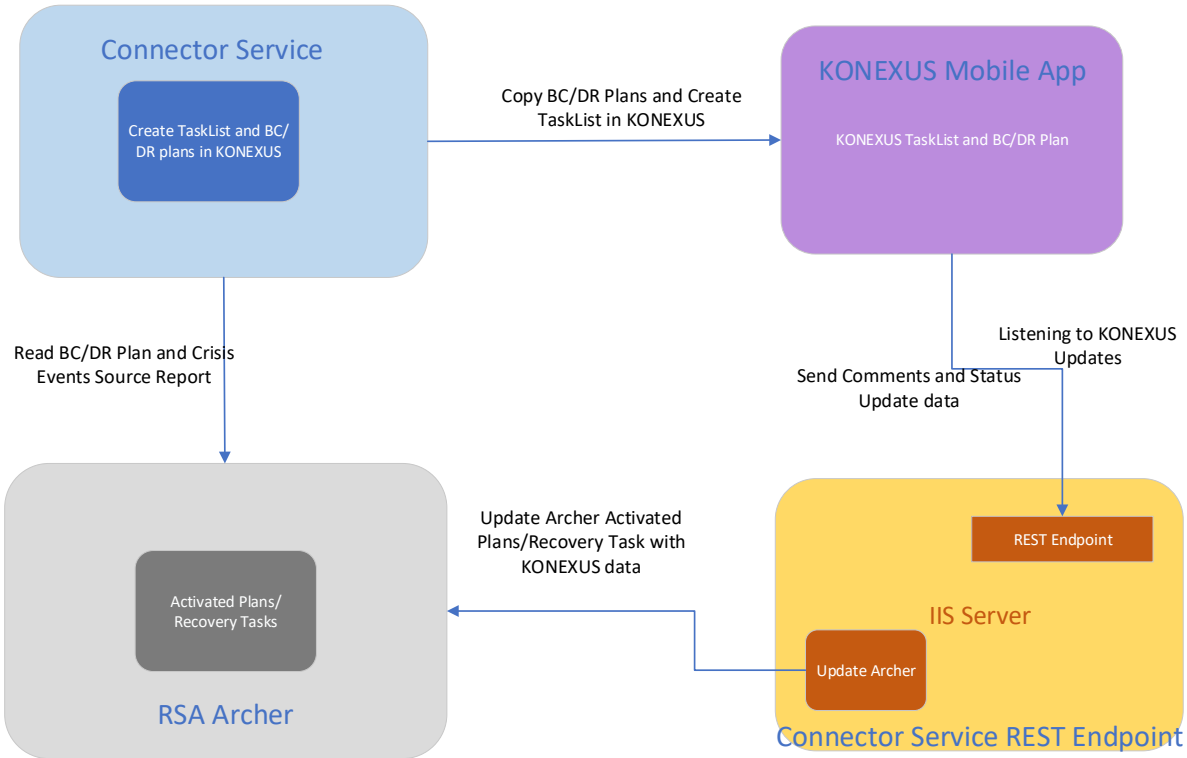
**Note:** Connector Service and Sync Service names are used interchangeably.

## Integration Diagram

The following diagram provides a high-level overview of the data flow process for the RSA Archer - KONEXUS Integration.

## SYSTEM INTEGRATION DETAILS



### Connector Service Creates KONEXUS SFTP Files

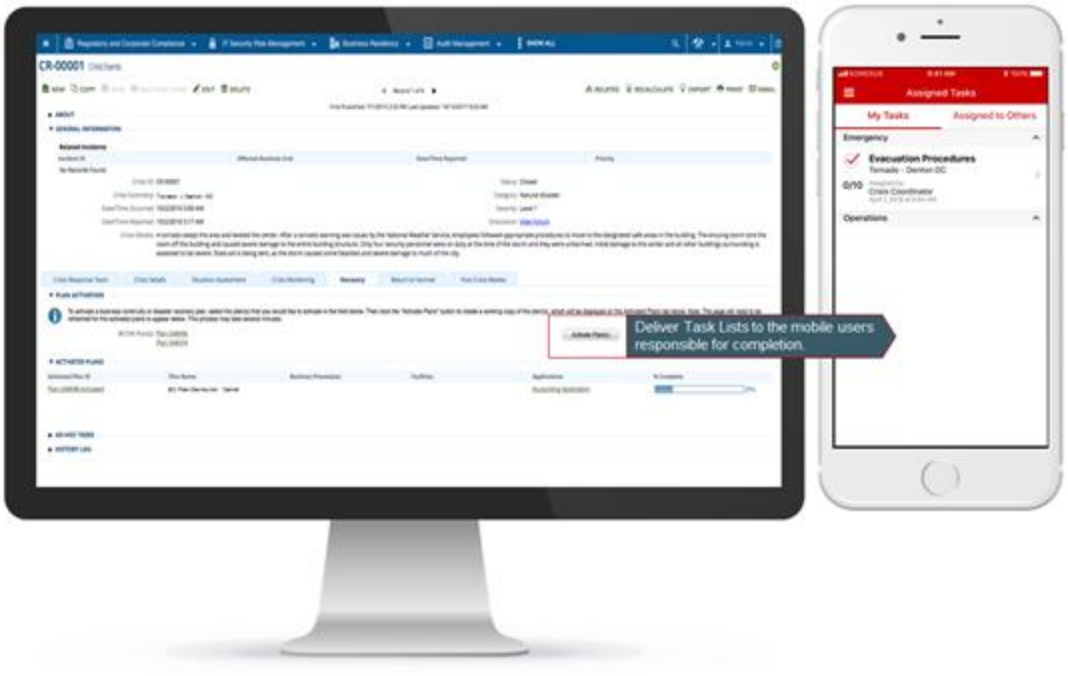
- These contain Archer's users, groups etc. This runs every morning at 2:00 A.M. MST by default and is configurable through “sftpimporttime” key present in ArcherTech.Services.SyncService.exe.config file and will upload it through sftp to KONEXUS server provided in the config file.
- Every morning at 4:00 A.M. MST KONEXUS runs the job, which will pick the sftp files uploaded by connector and will export the users and groups into the customer environment.
- This is vital for the onboarding process - Archer users will be automatically added to/removed from the customer's KONEXUS tenant.

### Connector Service Creates ‘Named Events/Incidents’ in the KONEXUS system

- These are automatically created via API when an Archer Crisis or Testing/Exercise is activated.
- The named events/incidents can be used when creating new alerts/polls in the KONEXUS system.
- They are removed from KONEXUS system when the Archer crisis is closed, or Testing/Exercise is “Approved” or “Rejected”.

### Connector Service Creates Task List in KONEXUS

- When a crisis is activated in Archer, the tasks contained in the plan's Recovery strategies are assigned to the task's 'assignees' and 'watchers’.
- Each task in the Archer system becomes a Tasklist in KONEXUS via API.
- The 'Recovery script' in an Archer task is free-form text - sometimes it has a large block of formatted text. If Recovery Task Script is created using numbered list or bulleted list, the connector converts each list item into a separate task in KONEXUS task list. This list becomes subtasks in Archer.
- Each task can have its own comments, and its own completion status. As part of adapting plans/recovery tasks to a more mobile-friendly experience, customers are encouraged to use this ‘numbered list’/’bullet list’ format in their task scripts. For more information on how to create task script in numbered/bullet lists, check Recovery task script help text.
- Sub-forms track the comments and completion status of each subtask.
- Archer also monitors task list activity that occurs in KONEXUS. Once the entire list of steps is complete (or skipped) in KONEXUS, the 'task' in Archer is marked complete (100%).
- Archer also supports a ‘skipped’ status for the Archer task.
- When a crisis is closed in Archer, the corresponding KONEXUS Task lists are removed from the app.




## RSA Archer Creates Plan Content in KONEXUS

- The content is organized in sections according to how plans/strategies/tasks/etc. are laid out in Archer's WebUI. There is a JSON (ArcherRecord.json) file that works as a layout manager. This will help in organizing Archer fields in particular sections in KONEXUS.
- There is a new report created “Archer - Konexus Integration BC/DR Plans Source Report” for the integration, which acts as a source to create BC/DR plan in KONEXUS. This allows a user to add/remove a field or change the structure of the plan in KONEXUS app content. This is the report that needs to be changed.
- To reflect the report changes or any update in the plan content the “Approved Plan Date” needs to be changed to today’s date.
- Only the approved plans will get copied and all activated plans appear under the “Activated” folder and not activated plans appear under “Not Activated” folder in the KONEXUS app.
- If there is an update in the BC/DR plan, the trigger point to update the plan in KONEXUS is to change the approval date to today’s date.
- The content is formatted in a way that can be easily viewed in the KONEXUS mobile app.
- Attachments are supported, so that when a plan has a doc file or a PDF, etc. that file accompanies the plan/content in KONEXUS.
- For this release, ‘everyone’ will have access to all the plan content in KONEXUS.

## Connector REST Endpoint Updates RSA Archer

- Connector REST Endpoint is a listener service that will listens to the KONEXUS events.
- Connector REST Endpoint updates RSA Archer’s Activated Plans Task with KONEXUS data.
    - Helps in updating the Task status.
    - Helps in adding comments to the Tasks.

# Chapter 2: Installation and Configuration

## Installation Overview

This section provides instructions for configuring the RSA Archer - KONEXUS Connector Service within the RSA Archer Platform.

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 documentation for all products to install the required components.

**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.

## Installing the Package

The following tasks detail how to import and install the "RSA_Archer_6.5_Business_Resiliency_Konexus_Integration_Install_Package.zip"

### 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

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

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.<br>**Important:** New objects should not be mapped. This icon should remain visible. The mapping process can proceed without mapping all the objects.<br><br>**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.

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.

In the Package Installation Log page, in the Object Details section, click View All Warnings.

## Installing and Configuring RSA Archer KONEXUS Integration

The RSA Archer - KONEXUS Integration has two components:

1. Connector REST Endpoint: must be deployed on IIS server and is responsible for listening to KONEXUS events and update Archer.
2. Connector Service: is a Windows service application and responsible to create Tasks and Plans in KONEXUS.

Extract the zip file **RSA Archer Konexus Integration.zip** to a location/folder.

### Step 1: Configuration of KONEXUS Connector REST Endpoint

The RSA Archer KONEXUS Connector REST Endpoint is a web application that needs to be deployed on IIS server.

Below are the steps to configure Connector REST Endpoint:

1. Extract the zip file **ConnectorRESTEndpoint.zip** to a location/folder.
2. Edit the instanceSection section of the XML configuration file “Web.config”.
   a. Navigate to the web application folder ConnectorRESTEndpoint and locate the Web.config file.
   b. Open Web.config file and provide the following information:

```
<appSettings>
    <add key="secretkey" value="[Secret Key Value]" />
</appSettings>
```

The XML configuration code below offers a configuration example.

```
<appSettings>
    <add key="secretkey" value="kd6epL382v4uWIUYtyyy77777yyyyyyyyyyy22" />
</appSettings>


<instanceSection>

   <instances>

       <instance archerBaseUrl="https://[YourArcherHostURL]/rsaarcher"
cacheFileNameAndPath="[cacheFileNameAndPath]"
cacheFileEncryptionPassphrase="[EncryptionPassphrase]"
useSslValidation="[true/false]" archerInstance="[InstanceName]"
archerUser="[UserName]" archerPassword="[Password]"/>

   </instances>
```

```
</instanceSection>
```

The description of each setting in Web.config file is as follows.

| Setting | Description |
|---|---|
| **secretkey** | Validate the incoming web hooks and prevent unauthorized requests. The purpose of the secret is to give the connector a mechanism to verify that requests are generated by KONEXUS and not a third-party pretending to be KONEXUS. The secret should only be known by the subscriber and KONEXUS. |
| **instanceSection** | This entry associates a custom configuration section with the assembly that will be used to process that section. This entry |
| **instances** | This section contains configuration information for each individually configured Archer instance. |
| **instance** | Each instance node defines the configuration for a single Archer Instance. The configuration file can contain as many instances are needed. |
| **archerBaseUrl** | The root URL for the RSA Archer instance from which information is pulled. |
| **cacheFileNameAndPath** | The flat file used to cache RSA Archer ID values. When the solution is started, values are looked up from the configured RSA Archer instance and stored in the cache file. This enables correctly referenced fields, modules, and other resources using IDs appropriate to the RSA Archer instance. |
| **cacheFileEncryptionPassphrase** | If provided, the cache file is encrypted using this setting as the passphrase, providing security for data at rest. |
| **useSslValidation** | When set to true, custom validation is used for the SSL certificate. This is necessary when using a self-signed certificate to avoid validation dialogs. |
| **archerInstance** | The name of the RSA Archer instance from which information is pulled. |
| **archerUser** | The name of the account used to pull information from RSA Archer. |
| **archerPwd** | The password for the account used to pull information from RSA Archer. |

The table below provides a description of each setting.

| Setting | Description and Example |
|---|---|
| **[Secret Key Value]** | Validate the incoming web hooks and prevent unauthorized requests.<br>**Note**: This Secret Key value should match with "secretkey" of Connector REST Endpoint. Otherwise it will not update RSA Archer to prevent unauthorized request. |
| **[YourArcherHostURL]** | RSA Archer host URL<br>Example: company.com or 10.20.30.40:99 |
| **[cacheFileNameAndPath]** | Cache file path and name<br>Example: C:\ArcherFiles \ArcherCache_RestEndpoint.txt |
| **[EncryptionPassphrase]** | Encryption pass phrase<br>Example: d0n7TryTh1s@h0m3! |
| **[true/false]** | True or false to validate SSL. When set to true, custom validation is used for the SSL certificate. This is necessary when using a self-signed certificate to avoid validation dialogs. |
| **[InstanceName]** | Instance name of your RSA Archer environment<br>Example: ArcherProd |
| **[UserName]** | Username of the account<br>Example: adminuser |
| **[Password]** | Password of the user account<br>Example: Password@123 |

3. Save and Close the Web.config file.
   **Note**: Changing the RSA Archer URL in the Config file requires the deletion of the previously used cache file.

### Logging

The solution makes use of a well-known logging framework called NLog. NLog allows for the creation of one or more log <target> entries, and one or more associated <logger> entries. The targets define potential "listeners" for log information, and the loggers define the rules associated with each of them, including log level. Although a sample config file is provided with the solution, a full discussion of the configuration file and its use is outside the scope of this document. For additional details, please see the **NLog documentation.**

4. Open NLog.config. Locate file target and provide the following information.
   **filename= "[logFilePath]"**
   Example: **fileName="c:\ArcherFiles\log\Archive \RESTEndpoint_Nlog.log"**
   Name of the file to write to. Provide name of the file to write to with the full path.

**archiveFileName="[archivelogFilePath]"**
Example: **archiveFileName="c:\ArcherFiles\log\Archive\RESTEndpoint_Nlog.{#}.log"**
Name of the file to be used for an archive. It contains a special placeholder {#} that will be replaced with a sequence of numbers depending on the archiving strategy. The number of hash characters used determines the number of numerical digits to be used for numbering files.

5. Go to IIS Server.
   i) Create a New Application.
   **Note:** In case you want to run the REST Endpoint application on the same port where Archer is running then create new application under Archer Site (hosted in IIS). Otherwise create a separate website in IIS.
   ii) Right Click on the Web Site -> Add Application…
   iii) Name the Alias Example - "ConnectorRESTEndpoint"
   iv) Choose the following folder for the path(where the application is copied)
   Example – "\ConnectorRESTEndpoint"
   v) Click "Connect as" and select - Application user(pass-through application)
   vi) Click on Browse Website link. Copy the web application link. You would need to provide this link in Connector Service config file in the next section.

## Configure SSL on Connector REST Endpoint

RSA Archer recommends using HTTPS configuration. But if the organization wants to use HTTP or SSL is already configured on the port used by the REST endpoint, they can skip this section.

The Connector REST Endpoint is responsible for listening to KONEXUS events and updating RSA Archer. For the communication to happen over SSL, the following steps need to be performed in the host where the Connector REST Endpoint is running.

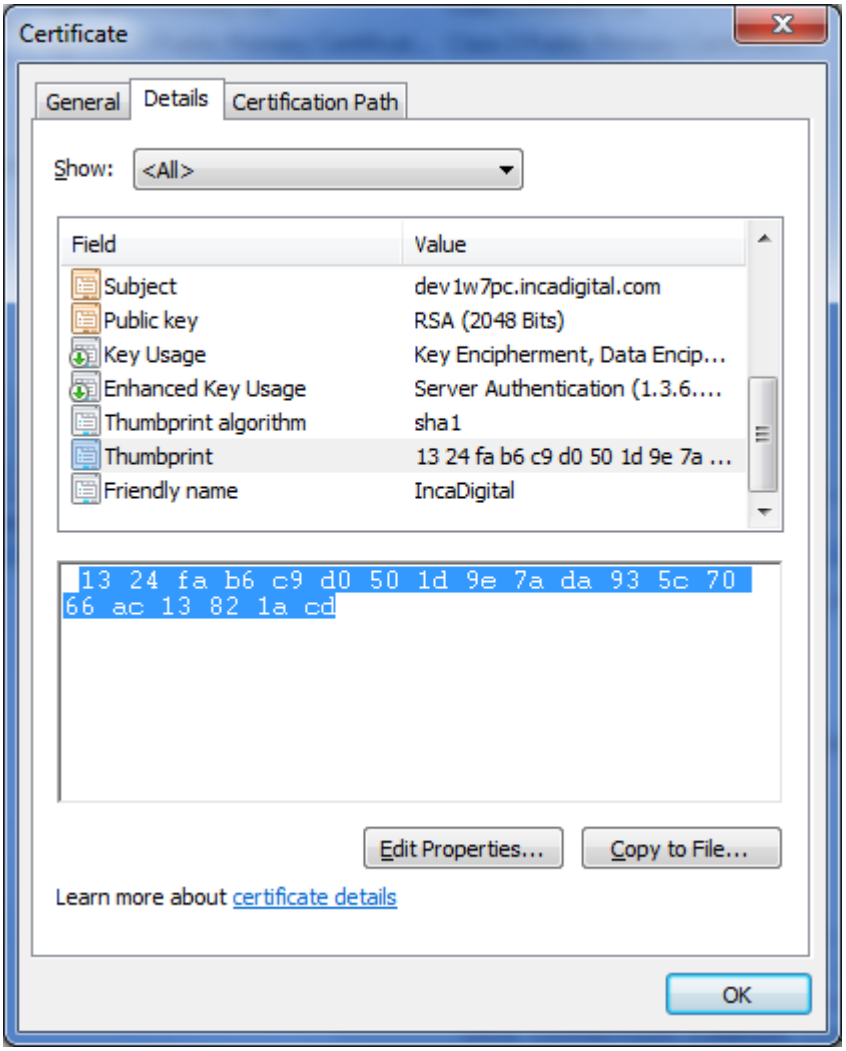
## Prerequisite

Signed certificate should be available.
**Note:** Signed certificate should be created from known Certificate Authority (CA) vendor. It should not be a self-signed certificate.

1. Follow these steps to install signed certificate into Trusted Root Certification Authorities using Microsoft Management Console (MMC): -
   a. Start -> Run -> "mmc"
   b. Select 'Add/Remove Snap-in' option from File menu
   c. Choose "Certificates" from Available Snap-in pane and Click Add>
   d. In the certificate snap-in window, choose "Computer Account" and Click Next>
   e. Click Finish [Make sure that option 'Local Computer: (the computer this console is running on)' is selected]
   f. Click OK in 'Add or Remove Snap-in' window
   g. Expand the "Certificates" in the left most pane Certificates > Trusted Root Certification Authorities > Certificates
   h. Right click on Certificates and select "All Tasks" > "Import…"
   i. In the wizard, click Next [Make sure that option 'Local Machine' is selected]

j. Choose Certificate to import the certificate
k. Repeat again for the "Personal" folder as well (so the Certificate is in two places)

2. Bind certificate to the TCP port where the connector REST endpoint is hosted. [Refer to the port number in "ArcherAlertSenseSubscriptionUrl" in **connector service** config file]. Also make sure this port is open to accept Inbound traffic.
3. Go to the installed certificate using Microsoft Management Console MMC). Double click on your certificate. Go to Details and scroll down to Thumbprint.
4. Copy the Thumbprint value of the certificate and remove all spaces from it (you can use Notepad). This value will be used later while running the command to bind the SSL certificate to the port in step 8.




5. Open command prompt and run following command to get the Application ID.
   **netsh http show sslcert**
   If the above command does not return any value, give any GUID. The Application ID doesn't really matter, it's just a GUID.

```
C:\>netsh http show sslcert

IP:port                 : 0.0.0.0:443
Certificate Hash        : 9aabf51a7686248ec48a4997f95e89bc9e9e366d
Application ID          : {214124cd-d05b-4309-9af9-9caa44b2b74a}
Certificate Store Name  : MY
Verify Client Certificate Revocation    : Enabled
Verify Revocation Using Cached Client Certificate Only    : Disabled
```

6. Open Command Prompt with elevated privileges (you get that by using the Run as Administrator option).
7. Run this command to bind the certificate you created to the port you are using.
   netsh http add sslcert ipport=0.0.0.0:**443** certhash=[cert-thumbprint] appid={[Application ID]}
8. Replace the [cert-thumbprint] and [Application ID] (including the square brackets) with the value you copied in steps 4 and 5.
   C:\> **netsh http add sslcert ipport=0.0.0.0:443 certhash=1324fab6c9d0501d9e7ada935c7066ac13821acd appid={214124cd-d05b-4309-9af9-9caa44b2b74a }**
   where certhash = SSL Thumbprint, and appid = Application ID

### Step-2: Installing the RSA Archer KONEXUS Connector Service

The RSA Archer - KONEXUS Connector Service is a Windows Service application. The solution includes an XML configuration file that allows for the specification of authentication credentials, along with other necessary details.

The below are the steps to configure Connector Service:

1. Extract the zip file **RSA Archer Konexus Connector Service.zip** to a location/folder.
2. Edit the appSettings section of the XML configuration file "**ArcherTech.Services.SyncService.exe.config**".

```
<appSettings>

    <add key="ArcherAlertSenseSubscriptionUrl"
value="https://[YourRESTEndPointHostURL]:[Port]"/>

    <add key="sftpimporttime" value="[SFTP Import Time IN MST Format]"/>

    <add key="planCopyPollingInterval" value="[Plan Copy Polling Interval in ms]" />

    <add key="taskCreatePollingInterval" value="[Create Task Polling Interval in ms]" />

    <add key="secretkey" value="[Secret Key Value]" />

</appSettings>
```

The XML configuration code below offers a configuration example.

```
<appSettings>

    <add key="ArcherAlertSenseSubscriptionUrl" value="https://partnersalescenter.com"/>

    <add key="sftpimporttime" value="02:00:00" />

    <add key="planCopyPollingInterval" value="60000" />

    <add key="taskCreatePollingInterval" value="30000" />

    <add key="secretkey" value="kd6epL382v4uWIUYtyyy77777yyyyyyyyyy22" />

</appSettings>
```

The configuration file also allows you to define Archer Instances, along with other necessary details.

```
<instanceSection>

    <instances>

      <instance archerBaseUrl="https://[YourArcherHostURL]/rsaarcher"
cacheFileNameAndPath="[cacheFileNameAndPath]"
cacheFileEncryptionPassphrase="[EncryptionPassphrase]" useSslValidation="[true/false]"
archerInstance="[InstanceName]" archerUser="[UserName]" archerPassword="[Password]"
alertSensePreAlphaApiUrl="[KONEXUS API Url]" AlertSenseAccessID="[KONEXUS Access ID]"
AlertSenseAccessSecret="[KONEXUS Access Secret]" alertSenseApiKey="[KONEXUS API Key]"
sftphost="[SFTP Server/Host]" sftpdestination ="[SFTP Server File Destination Folder]"
sftpusername="[SFTP User Name]" sftppassword="[SFTP Password]" sftpport="[SFTP Port]" />
```

The XML configuration code below offers a configuration example.

```
<instance archerBaseUrl="https://localhost/archer"
cacheFileNameAndPath="C:\ArcherFiles\ArcherCacheFile_Service.txt"
cacheFileEncryptionPassphrase="d0n7TryTh1s@h0m3!" useSslValidation="false"
archerInstance="archer" archerUser="guptar10" archerPassword="Password1-2"
alertSensePreAlphaApiUrl="https://content.alertsense.com" AlertSenseAccessID="rsa"
AlertSenseAccessSecret="d9a1f6ab-4e52-476b-bd13-d8de1fdd87f8" alertSenseApiKey="c360f4d5-
61d5-4717-asba-2514b412beed" sftpdestination="/import" sftphost="upload.alertsense.com"
sftpusername="rsa" sftppassword="3U7A4wyHxfBpyC8w" sftpport="22" />
```

The description of each setting in ArcherTech.Services.SyncService.exe.config file is as follows.

| Setting | Description |
|---|---|
| **ArcherAlertSenseSubscriptionUrl** | REST Endpoint Host URL where the application is running |
| **sftpimporttime** | SFTP import time in Mountain Standard time |
| **planCopyPollingInterval** | BC/DR Plan copy Polling Interval in milliseconds |

| Setting | Description |
|---|---|
| **taskCreatePollingInterval** | Create Task List Polling Interval in milliseconds |
| **secretkey** | Validate the incoming web hooks and prevent unauthorized requests. The purpose of the secret is to give the connector a mechanism to verify that requests are generated by KONEXUS and not a third-party pretending to be KONEXUS. The secret should only be known by the subscriber and KONEXUS. |
| **archerBaseUrl** | The root URL for the RSA Archer instance from which information is pulled. |
| **cacheFileNameAndPath** | The flat file used to cache RSA Archer ID values. When the solution is started, values are looked up from the configured RSA Archer instance and stored in the cache file. This enables correctly referenced fields, modules, and other resources using IDs appropriate to the RSA Archer instance. |
| **cacheFileEncryptionPassphrase** | If provided, the cache file is encrypted using this setting as the passphrase, providing security for data at rest. |
| **useSslValidation** | When set to true, custom validation is used for the SSL certificate. This is necessary when using a self-signed certificate to avoid validation dialogs. |
| **archerInstance** | The name of the RSA Archer instance from which information is pulled. |
| **archerUser** | The name of the account used to pull information from RSA Archer. |
| **archerPwd** | The password for the account used to pull information from RSA Archer. |
| **alertSensePreAlphaApiUrl** | KONEXUS content base Url |
| **AlertSenseAccessID** | KONEXUS Access ID |
| **AlertSenseAccessSecret** | KONEXUS Access Secret Key |
| **alertSenseApiKey** | KONEXUS API key |
| **sftpdestination** | KONEXUS destination folder where the user/group csv files needs to be copied. |
| **sftphost** | KONEXUS SFTP host name where the user/group csv files needs to be copied. |
| **sftpusername** | KONEXUS SFTP user name |
| **sftppassword** | KONEXUS SFTP Password |
| **sftpport** | KONEXUS SFTP port |

The table below provides a description of each setting.

| Setting | Description and Example |
|---|---|
| **[YourRESTEndpointHostURL]** | Host URL where the Connector REST EndPoint is running.<br>https://[YourRESTEndPointHostURL]:[port]<br><br>Example1: https://partnersalescenter.com It runs on default port 443<br>Example2: https://partnersalescenter.com**:9090** It runs on dedicated opened port 9090<br>**Note: The port number used in the above URL should be configured to accept the inbound traffic.** |
| **[SFTP Import Time IN MST Format]** | Time in Mountain Standard Time when the Connector service will create Users/groups csv file from Archer and upload it to KONEXUS system via sftp CSV file be created to<br>the same folder where the service is running and then uploaded to sftp site to get picked by KONEXUS Job for exporting the users into KONEXUS system.<br>Example: 02:00:00 |
| **[Plan Copy Polling Interval in ms]** | BC/DR Plan copy Polling Interval in milliseconds. The default value is 60 seconds. This is the time gap after which connector service will check if there is any plan to update or create. **Recommended value is not less than 60 seconds** depending on the how frequently plans will get created/updated.<br>Example: 60000 |
| **[Create Task Polling Interval in ms]** | Create Task List Polling Interval in milliseconds. The default value is 60 seconds. This is the time gap after which connector service will check if there is any task to create. **Recommended value is not less than 30 seconds**.<br>Example: 30000 |
| **[Secret Key Value]** | Validate the incoming web hooks and prevent unauthorized requests. **Note**: This Secret Key value should match with "secretkey" of Connector REST Endpoint. Otherwise it will not update RSA Archer to prevent unauthorized request. |
| **[YourArcherHostURL]** | RSA Archer host URL<br>Example: company.com or 10.20.30.40:99 |
| **[cacheFileNameAndPath]** | Cache file path and name<br>Example: c:/ArcherFiles/logs/ArcherCacheFile_Service.txt |
| **[EncryptionPassphrase]** | Encryption pass phrase<br>Example: d0n7TryTh1s@h0m3! |
| **[true/false]** | True or false to validate SSL<br>Example: false |

| Setting | Description and Example |
|---|---|
| **[InstanceName]** | Instance name of your RSA Archer environment<br>Example: ArcherProd<br>**Note:** Instance name is case sensitive. |
| **[UserName]** | Username of the account<br>Example: adminuser |
| **[Password]** | Password of the user account<br>Example: Password@123 |
| **[KONEXUS API Url]** | KONEXUS content base Url<br>Example: https://content.alertsense.com |
| **[KONEXUS Access ID]** | KONEXUS Access ID<br>Example: rsa |
| **[KONEXUS Access Secret]** | KONEXUS Access Secret Key<br>Example: d9a1f6ab-4e52-476b-bd13-d8de1fdd87f8 |
| **[KONEXUS API Key]** | KONEXUS API key<br>Example: c360f4d5-61d5-4717-asba-2514b412beed |
| **[SFTP Server/Host]** | KONEXUS destination folder where the user/group csv files needs to be copied<br>Example: upload.alertsense.com |
| **[SFTP Server File Destination Folder]** | KONEXUS SFTP host name where the user/group csv files need to be copied.<br>Example: /import |
| **[SFTP User Name]** | KONEXUS SFTP user name<br>Example: rsa |
| **[SFTP Password]** | KONEXUS SFTP Password<br>Example: 3U7A4wyHyhBpyC8w |
| **[SFTP Port]** | KONEXUS SFTP port<br>Example: 22 |

1. Save and Close the ArcherTech.Services.SyncService.exe.config file.

   **Note:** Changing the RSA Archer URL in the Config file requires the deletion of the previously used cache file.

2. If you need to manage multiple Archer instances, add a separate <instance> tag for each Archer instance. For example:

```
<instanceSection>

    <instances>
```

```
            <instance1 …. />
            <instance2 …. />

        <instances>

    <instanceSection>
```

3. Open NLog.config. Locate file target and provide the following information.

   `filename= "[logFilePath]"`

   Example: `fileName="c:\ArcherFiles\SyncService_Nlog.log"`

   Name of the file to write to. Provide name of the file to write to with the full path.

   `archiveFileName="[archivelogFilePath]"`

   Example: `archiveFileName="c:\ArcherFiles\log\Archive\SyncService_Nlog.{#}.log"`

   Name of the file to be used for an archive. It contains a special placeholder {#} that will be replaced with a sequence of numbers depending on the archiving strategy. The number of hash characters used determines the number of numerical digits to be used for numbering files.

4. Right click the file “InstallSyncService.bat” and Run as Administrator. This will create ArcherTech.Services.SyncService in Windows. Start this service. If there are any errors while installing the service please refer to the ArcherTech.Services.SyncService.InstallLog file.
   To Uninstall the Sync Service, right click the file “UnInstallSyncService.bat” and Run as Administrator. This will uninstall the service.

## Security Consideration

1. Use HTTPS/TLS for secured connection between the Connector service and KONEXUS /Archer.
2. Run the Sync service with the least privileged account (Logon Service permission).

## Security

Batch files are provided that will encrypt the appSettings and instanceSection configuration sections. .NET is able to read the encrypted sections at runtime, so the decryption batch file is provided in case the encrypted sections need to be edited. Copy these batch files to the deployment folder and edit the frameworkPath and originalPath to point to the correct locations. FrameworkPath should point to the location of your .NET framework (by default this will be C:\Windows\Microsoft.NET\Framework\v4.0.30319). OriginalPath should point to the deployment folder containing the config file you are encrypting and the associated binaries. The batch file must be run as administrator to succeed. It will be necessary to change the target for each file to be encrypted or decrypted. The contents of Encrypt.bat and Decrypt.bat are included here for reference.

## Encrypt.bat

```
@echo off

set frameworkPath=C:\Windows\Microsoft.NET\Framework\v4.0.30319
set originalPath=["Directory path to the config file"]

if "%1"=="" (set originalFileName=ArcherTech.Services.SyncService.exe.config) else (set originalFileName=%1)
cd %frameworkPath%
echo.
@echo This batch file will encrypt the instanceSection and appSettings sections in %originalPath%\%originalFileName%
@echo Saving original file as %originalPath%\%originalFileName%.original
copy %originalPath%\%originalFileName% %originalPath%\%originalFileName%.original
rename %originalPath%\%originalFileName% web.config
echo.
@echo encrypting appSettings...
aspnet_regiis -pef "appSettings" %originalPath% -prov "DataProtectionConfigurationProvider"

@echo preparing files for custom config section encryption
copy %originalPath%\ArcherTech.Services.SyncService.exe %frameworkPath%
echo.

aspnet_regiis -pef "instanceSection" %originalPath% -prov "DataProtectionConfigurationProvider"

rename %originalPath%\web.config %originalFileName%
del %frameworkPath%\ArcherTech.Services.SyncService.exe
pause
```

## Decrypt.bat

```
@echo off

set frameworkPath=C:\Windows\Microsoft.NET\Framework\v4.0.30319
set originalPath=["Directory path to the config file"]

if "%1"=="" (set originalFileName=ArcherTech.Services.SyncService.exe.config) else (set originalFileName=%1)
cd %frameworkPath%
echo.
@echo This batch file will decrypt the instanceSection and appSettings sections in %originalPath%\%originalFileName%
@echo Saving original file as %originalPath%\%originalFileName%.original
copy %originalPath%\%originalFileName% %originalPath%\%originalFileName%.original
rename %originalPath%\%originalFileName% web.config
echo.
@echo decrypting appSettings...
aspnet_regiis -pdf "appSettings" %originalPath%
echo.
@echo preparing files for custom config section decryption
copy %originalPath%\ArcherTech.Services.SyncService.exe %frameworkPath%
echo.
@echo Decrypting instanceSection...
aspnet_regiis -pdf "instanceSection" %originalPath%
echo.
@echo cleaning up files from custom config section decryption
rename %originalPath%\web.config %originalFileName%
del %frameworkPath%\ArcherTech.Services.SyncService.exe
pause
```

# Troubleshooting Guidelines

## Configuration File (ArcherTech.Services.SyncService.exe.config)

- Assure the values in the configuration file match your RSA Archer environment.
- Do not include default.aspx in the RSA Archer URL.
- The RSA Archer instance name is case sensitive.
- Each time you change the RSA Archer URL in Config file, you must delete the previously used cache file.
- Assure that dedicated, active RSA Archer user account credentials use the configuration file.

## Others

- Task 'assignees' and the 'watchers’ are the mandatory fields. If activated task does not have both 'assignees' and the 'watchers’ in Archer, the task list won’t get created in KONEXUS.

- SFTP user sync happens every morning 4.30AM MST. In case a new user is added that user should not be made 'assignees' or the 'watchers' to the activated task until SFTP import is completed and that user is exported to KONEXUS system. Otherwise task creation will fail.
- To run the SFTP import make sure sftp port is opened so that connector service can upload the users/group csv files to the KONEXUS sftp host.
- Secret Key parameter defined in Connector service config file and Connector REST Endpoint config file is not mandatory. If not defined the REST Endpoint service will use default secret key to verify requests are generated by KONEXUS
- Values of Secret key defined in Connector service config file and Connector REST Endpoint config file should match. Otherwise Connector REST Endpoint will not update RSA Archer to prevent unauthorized request.

## Known Issues

- If some unordered data or instruction is provided in "Recovery task script" field followed by an ordered list (numbered list), KONEXUS ignores the data provided ahead of the ordered list data. This would cause loss of data.
- Multiple Plan Target values should be separated by commas or semicolons in the BC/DR record in KONEXUS.
- Other text value is not visible in Loss Type field of recovery strategy in the BC/DR record in KONEXUS.

## Frequently Asked Questions

**Why I am unable to see my task list in KONEXUS app?**

1. The Archer user is not mapped to KONEXUS system. To fix this make sure SFTP sync happens and the user is exported into KONEXUS system.
2. Task 'assignees' and the 'watchers' are the mandatory fields. If activated task does not have both 'assignees' and the 'watchers' in Archer, the task list will not get created in KONEXUS.

**Why isn't my Archer task is being split into multiple subtasks in KONEXUS?**

The 'Recovery script' in an Archer task is free-form text - sometimes it has a large block of formatted text. If Recovery Task Script is created using numbered list or bulleted list, the connector converts each list item into a separate task in KONEXUS task list. This becomes subtasks in Archer.

**Why I am unable to see Plan Content in KONEXUS?**

We only copy approved plans in KONEXUS. To see BC/DR plans in KONEXUS app, make sure plans are approved in Archer.

**Why I am unable to see updates made to the Archer BC/DR plan in KONEXUS app?**

The trigger point to update the Archer plans in KONEXUS is approval date. If the approval date is lesser than the copy date, connector will not update the plans in KONEXUS.

**I have added/removed fields or changed the structure of the BC/Plan source report "Archer - KONEXUS Integration BC/DR Plans Source Report" but can't see the changes reflected back in the KONEXUS App.**

When we add or remove a field in "Archer – Konexus Integration BC/DR Plans Source Report", it does not reflect in KONEXUS app with immediate effect. For the change to get reflected in the report, the user will need to change the approval date of Plans. This change will get reflected only for those plans with updated approval dates. The other plans will populate the same unchanged structure until the plans are approved.

**Why are my updates in KONEXUS task list not getting mirrored back in Archer?**

Make sure the host where the connector service is running is accessed by KONEXUS System and the port number defined in "ArcherAlertSenseSubscriptionUrl" is not blocked.

## Certification Environment

Date tested: August 2019

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| RSA Archer Platform | 6.5 | Virtual Appliance |

## Revision Notes

| Document Version | Published Date | Notes |
|---|---|---|
| 1.1 | August, 2019 | This version of integration handle HTTPS configuration in a better way. Previous version of integration had limitation that RSA Archer and Connector Service cannot be configured to run on the same host and port. The new version allows to share the port with Archer. Connector REST endpoint can be deployed on the same host and port.<br><br>The version also uses NLog framework for better logging.<br>Previous version of integration was not using any logging framework and writing it to one log file which will over time, become quite large and difficult to work with. The idea is to use NLog which is much more configurable.<br><br>The new version also validates the incoming web hooks and prevent unauthorized requests. The purpose of the secret is to give the connector a mechanism to verify that requests are generated by KONEXUS and not a third party pretending to be KONEXUS. |