Icon

Description automatically generated



Archer®

Archer Version: 2024.09 or later

Implementation Guide

Bitsight - Archer VRM Integration

Version 1.0

Revision 4/30/2025



Table of Contents

[Release Notes 3](#_Toc196717866)

[Release 1.0 3](#_Toc196717867)

[Chapter 1: Overview of Bitsight VRM 4](#_Toc196717868)

[About Bitsight 4](#_Toc196717869)

[Key Features and Benefits 4](#_Toc196717870)

[Prerequisites (ODA and system requirements) 4](#_Toc196717871)

[Compatible Use Cases and Applications 4](#_Toc196717872)

[Related Applications 4](#_Toc196717873)

[Impacted Use Case(s) 5](#_Toc196717874)

[Impacted Fields (Integrations only) 5](#_Toc196717875)

[Additional Resources 5](#_Toc196717876)

[Chapter 2: Bitsight VRM Components 5](#_Toc196717877)

[Architecture Diagram 5](#_Toc196717878)

[Swim Lane Diagram 6](#_Toc196717879)

[Applications 7](#_Toc196717880)

[Personas and Access Roles 7](#_Toc196717881)

[Installation Overview 8](#_Toc196717882)

[Step 1: Prepare for the Installation 8](#_Toc196717883)

[Step 2: Install the Package 8](#_Toc196717884)

[Step 3: Set up Integration Applications 8](#_Toc196717885)

[Step 4: Test the Installation 8](#_Toc196717886)

[Installing the Package 8](#_Toc196717887)

[Task 1: Back Up Your Database 8](#_Toc196717888)

[Task 2: Import the Package 8](#_Toc196717889)

[Task 3: Map Objects in the Package 9](#_Toc196717890)

[Task 4: Install the Package 11](#_Toc196717891)

[Task 5: Review the Package Installation Log 12](#_Toc196717892)

[Manual Changes in Third Party Profile 13](#_Toc196717893)

[Setup Integration Applications 19](#_Toc196717894)

[Task 1: Create Archer API User Account 19](#_Toc196717895)

[Task 2: Create Bitsight API Token 19](#_Toc196717896)

[Task 3: Configuring Integration between Archer and Bitsight 20](#_Toc196717897)

[Task 4: Optional: Configure the nightly.bat file 22](#_Toc196717898)

[Task 5: Setup Job Scheduling 22](#_Toc196717899)

[Task 6: Security and Hardening 25](#_Toc196717900)

[Bitsight Token 25](#_Toc196717901)

[Least Privilege Model 25](#_Toc196717902)

[API Integration Code Security 25](#_Toc196717903)

[Chapter 5: Upgrading Bitsight VRM Integration 25](#_Toc196717904)

[Chapter 6: Using Bitsight VRM Integration 25](#_Toc196717905)

[Additional Configuration 25](#_Toc196717906)

[Access Groups and Roles 26](#_Toc196717907)

[Bitsight Licensing Overview 26](#_Toc196717908)

[Bitsight Dashboard 27](#_Toc196717909)

[High Level Process Overview 28](#_Toc196717910)

[Existing Bitsight VRM Customers (initial setup) 28](#_Toc196717911)

[Monitor a New Vendor 28](#_Toc196717912)

[Appendix A: Certification Environment 29](#_Toc196717913)

[Appendix B: Access Considerations 29](#_Toc196717914)

[Appendix C: Known Future Improvements 29](#_Toc196717915)

[Appendix D: Frequently Asked Questions (FAQ) 30](#_Toc196717916)

# Release Notes

## Release 1.0

Version 1.0 is a new integration between Archer and Bitsight VRM functionality.

# Chapter 1: Overview of Bitsight VRM

## About Bitsight

Bitsight is a leading cyber threat intelligence platform that transforms how organizations manage cyber risk. By continuously monitoring and analyzing externally observable data, Bitsight delivers objective, evidence-based cyber threat intel that help businesses make informed decisions about risk management, vendor assessment, and regulatory compliance. Trusted by security and risk professionals worldwide, Bitsight empowers organizations to gain visibility into their own security posture and that of their third-party ecosystem.

The Bitsight and Archer integration brings cyber risk data from Bitsight to the Archer Platform enabling a mapping between the Bitsight security rating and related information for a specific company with vendor catalog and risk management information that resides in the Archer.

## Key Features and Benefits

Key benefits

With the offering, you will be able to:

* Ability to quickly add Bitsight VRM data into Third Party Profiles
* Initiate creation of new Bitsight VRM company to monitor
* Nightly updates of risk ratings and key VRM details to manage risk
* Nightly updates of company VRM findings

## Prerequisites (ODA and system requirements)

|  |  |
| --- | --- |
| Components | Prerequisites |
| Archer Solution Area(s) | Archer Third Party Governance |
| Archer Use Case(s) | Archer Third Party Catalog |
| Archer Applications | Third Party Profile |
| Uses Custom Application | No, but one new questionnaire is deployed |
| Requires On-Demand License | No |
| Archer Requirements | Archer Version: 2024.09 (Build: 6.15.00302.10262) and later |
| Partner/Vendor Requirements | Valid Bitsight VRM subscription is required. |

## 

## Compatible Use Cases and Applications

### Related Applications

|  |  |  |
| --- | --- | --- |
| **Application** | **Use Case** | **Primary Purpose(s) of the Relationship** |
| Third Party Profile | Third Party Catalog | * Use the existing Third Party Profile record to store and leverage the Bitsight VRM data to facilitate the monitoring of your vendors. |

### Impacted Use Case(s)

|  |
| --- |
| Archer Use Case(s) |
| Third Party Catalog |

## Impacted Fields (Integrations only)

A single cross reference between Third Party Profiles and the Bitsight VRM Findings questionnaire will link the two records together. All other integration data is mapped to the new Bitsight VRM Findings questionnaire.

## Additional Resources

The following additional resources are available for this offering:

* [Bitsight Website](https://www.bitsight.com/)
* [Tutela Solutions Website](https://www.tutela-solutions.com/)

# Chapter 2: Bitsight VRM Components

## Architecture Diagram

Below is the architecture of the Bitsight VRM solution and explanation of the components.

**Third Party Profile (TPP)** stores Bitsight VRM information with new fields. If you are already monitoring Bitsight VRM vendors, simply adding the Bitsight VRM Domain will begin the syncing process. To monitor a new vendor, adding the vendor domain in Archer will initiate the process to add a vendor to monitor in the Bitsight VRM Portal.

The **Bitsight VRM Findings** questionnaire stores finding information for your Bitsight VRM vendors. The data is updated nightly to track the issue and status. Findings are shown on the related TPP record.

A diagram of a diagram

AI-generated content may be incorrect.

## Swim Lane Diagram

The following information describes the swim lane diagram further below. Please refer to the diagram for a visual understanding of the high level process.

The **Initial Setup** process starts with creating or updating a record in Third Party Profile and specifying the web site domain of that company in the **Bitsight VRM Domain** field. A nightly scheduled job identifies records with new vendors and attempts to create the vendor record in Bitsight VRM.

The **Update Third Party Profile Bitsight VRM Data** process retrieves a list of Third Party Profiles that have a **Bitsight VRM Domain**. The integration application requests the Bitsight VRM data via API for each of the companies. The integration application then assembles all the data and updates the Archer Third Party Profile Bitsight VRM fields.

While not shown in the diagram, the process also ensures alignment between the values lists between Archer and Bitsight for the **Bitsight VRM Lifecycle** and **Bitsight VRM Tags** fields and will make updates if necessary.

The **Update Bitsight VRM Findings in Archer** process retrieves a list of Third Party Profiles that have a **Bitsight VRM Domain**. The integration application requests Bitsight VRM finding data via API for each of the companies and iterates all findings. Next, the integration application obtains the current Finding data from Archer in the Bitsight VRM Findings questionnaire. The integration application then identifies any differences, assembles all the data, and updates the Archer Bitsight VRM Findings records.

While not shown in the diagram, the process also ensures alignment between the values lists between Archer and Bitsight for the **Finding Status** field and will make updates if necessary.

The following diagram shows the general workflow of the solution:

*Hint: Using the zoom feature, you can zoom in closer to display all the components clearly.* A screenshot of a computer screen

AI-generated content may be incorrect.

## Applications/Questionnaires

The following applications and questionnaires are used in the Bitsight VRM solution.

|  |  |
| --- | --- |
| Application | Description |
| Third Party Profile | Third Party Profile is where you specify the web site domain of the Bitsight VRM company which is used for syncing purposes with Bitsight VRM’s API to bring data into Archer on a nightly basis. |
| Bitsight VRM Findings | The Bitsight VRM Findings questionnaire stores findings information from Bitsight’s API. Updates are made when differences are found on a nightly basis. |

## Personas and Access Roles

The following table describes the functions that make up the application’s organization roles. Depending on the organization of your company, these functions and responsibilities may vary.

|  |  |
| --- | --- |
| Function | Description |
| Risk Manager | The role your organization uses to manage Third Party Profiles with access to update the Bitsight VRM Domain field. |
| Bitsight VRM API Users | Provides access to one API user account used to update the Third Party Profile Bitsight VRM fields and create/update the Bitsight VRM Findings questionnaire records. |

# Chapter 3: Installing Bitsight VRM

## Installation Overview

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 2024.09 (Build: 6.15.00302.10262) or later
2. 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](#InstallAppPackage) for complete information. Manual configuration is also necessary to properly setup the solution.

## Step 3: Set up Integration Applications

The Bitsight VRM integration utilizes scheduled integration applications. See [Setting Up Integration Applications](#SettingUpDataFeeds) for complete information.

*Note: Archer Data Feeds may be available in a future version, however they will not be available for SaaS or Hosted customers due to the restrictions Archer IRM has regarding JavaScript Transporter Data Feeds which were not directly developed by Archer IRM.*

## Step 4: Test the Installation

Test the application according to your company standards and procedures, to ensure that the use case works with your existing processes.

## Installing the Package

### 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. Archer 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.

### Task 2: Import the Package

1. Go to the Install Packages page.
   1. From the menu bar, click .
   2. 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.

Note: It is not necessary to include the “Questionnaire Comments” sub-form in the installation and is not used in the solution.

### 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.

1. 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. |

1. 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 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:
2. In the toolbar, click Auto Map.
3. 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. |

1. 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.

1. 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.

1. Verify that all other objects are mapped correctly.
2. (Optional) To save your mapping settings so that you can resume working later, see "Exporting and Importing Mapping Settings" in the
3. Archer Online Documentation.
4. Once you have reviewed and mapped all objects, click .
5. 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.

### 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.

1. Go to the Install Packages page.
   1. From the menu bar, click .
   2. 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.

1. 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.

1. 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.

1. 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.
2. Click Install.
3. Click OK.

### Task 5: Review the Package Installation Log

1. Go to the Package Installation Log tab of the Install Packages page.
   1. From the menu bar, click .
   2. Under Application Builder, click Install Packages.
   3. 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.

# Manual Changes in Third Party Profile

The steps below outline the manual changes needed in the Third Party Profile application to support the integration. Because there are changes to a core Archer application, Archer prohibits providing a package that updates core applications.

Your organization may enhance the Third Party Profile with additional calculations, private fields, record permissions, DDEs, or notifications to leverage the Bitsight VRM information.

**Important Note:** It is critical the fields below be created with the exact name and values outlined below to ensure proper functionality. The fields can be placed anywhere on the application, but the naming is critical for the integration applications.

* + 1. Manage the **Third Party Profile** application in Application Builder
    2. Properties:
       1. Administration:
          1. Configuration Administrators:

Add group: Bitsight VRM API Accounts

Note: this allows management of the list values. Optionally you can update the **Bitsight VRM API** access role with CRUD access to the following values lists:

Bitsight VRM Lifecycle

Bitsight VRM Tags

* + - * 1. Content Administrators:

Add group: Bitsight VRM API Accounts

* + - 1. Save
    1. Create a new tab in the Default Tab Set
       1. Name: Risk Assessments (or whatever name you prefer)
       2. Placement/Order: Your preference
    2. On the **Risk Assessments** tab (or wherever you prefer), create the following objects and fields:
       1. Create a new section:
          1. Name: Bitsight VRM
       2. Create a new text field:
          1. Name: Bitsight VRM Domain
          2. Display Control: Text Field
          3. Suggested help text: Enter the domain name of the company you would like to track. *Example: microsoft.com*
       3. Create a new values list field:
          1. Name: Bitsight VRM Lifecycle
          2. Options: Dropdown
          3. Values: Empty since they will be populated and automatically updated by the API integration.
       4. Create a new numeric field:
          1. Name: Bitsight Security Rating
          2. Configuration:

Decimal Places: None

* + - 1. Create a new numeric field:
         1. Name: Bitsight VRM Impact Score
         2. Configuration:

Decimal Places: None

* + - 1. Create a new numeric field:
         1. Name: Bitsight VRM Trust Score
         2. Configuration:

Decimal Places: None

* + - 1. Create a new numeric field:
         1. Name: Bitsight VRM Risk Score
         2. Configuration:
      2. Decimal Places: None
      3. Create a new numeric field:
         1. Name: Bitsight VRM Requirements Completion %
         2. Configuration:

Decimal Places: None

Minimum Value: 0

Maximum Value: 100

*Optional:* Suffix: %

* + - 1. Create a new date field:
         1. Name: Bitsight VRM Requirements Due Date
         2. Display Control: Text Box - Date
      2. Create a new numeric field:
         1. Name: Bitsight VRM Review Year
         2. Options:

Format the numeric value using thousand separators: Unchecked

* + - * 1. Configuration:

Decimal Places: None

Minimum Value: 2000

Maximum Value: 2040

* + - 1. Create a new text field:
         1. Name: Bitsight VRM GUID
         2. Display Control: Text Field
      2. Create a new text field:
         1. Name: Bitsight GUID
         2. Display Control: Text Field
      3. Create a new text field:
         1. Name: Bitsight VRM Deep Link
         2. Display Control: Text Area
      4. Create a new date field:
         1. Name: Bitsight VRM Last Updated Date
         2. Display Control: Text Box - Date
      5. Create a new values list field:
         1. Name: Bitsight VRM Tags
         2. Display Control: Values Popup
         3. Configuration:

Minimum Selections: No Minimum

Maximum Selections: No Maximum

* + - * 1. Values: Empty since they will be populated and automatically updated by the API integration.
        2. When adding to the layout, we suggest setting the Row Span setting to 4 since multiple tags can be selected to improve the display to the user.
      1. The **Bitsight VRM Findings** cross-reference should already exist from package creation and can be dragged onto layout under all the other fields.

Example/suggested layout after creating all the fields:

A screenshot of a web page

AI-generated content may be incorrect.

* 1. **Create new report in Third Party Profile**
     1. Name: Bitsight VRM Listing
     2. Selected Fields (order below is suggested, but feel free to configure as you wish):
        1. Third Party Profile
        2. Bitsight VRM Domain
        3. Bitsight Security Rating
        4. Bitsight VRM Last Update Date
        5. Bitsight VRM Lifecycle
        6. Bitsight VRM Impact Score
        7. Bitsight VRM Trust Score
        8. Bitsight VRM Risk Score
        9. Bitsight VRM Requirements Completion %
        10. Bitsight VRM Requirements Due Date
        11. Bitsight VRM Review Year
        12. Bitsight VRM Tags
        13. Bitsight VRM Deep Link
        14. Bitsight GUID
        15. Bitsight VRM GUID
        16. Bitsight VRM Findings
     3. Filters:
        1. None - *Unless you only want to show TPPs where a Bitsight VRM Domain is not empty*
     4. Sorting:
        1. Third Party Name - Ascending
     5. Display Format: Column - Flat
     6. Record Count: Return All
     7. Results Per Page: 50
     8. Enable Inline Edit: Checked
     9. Search and Save report
        1. Permissions: Global to Everyone
  2. Consider adding this report to one of your existing dashboards.

# Setup Integration Applications

## Task 1: Create Archer API User Account

*Below are some suggested names and settings. However, please follow any organizational standards and simply take note of the differences when configuring the JavaScript applications.*

1. Account Settings:
2. First Name: dfm\_BitsightVRMAPINightly
3. Last Name: API
4. User Name: dfm\_BitsightVRMAPINightly
5. Security Parameter: Data Feed and API Parameter (or whatever parameter your company uses with non-expiring passwords)
6. Password: Whatever secure password you want
7. Force Password Change: unchecked
8. Groups: Bitsight VRM API Accounts

## Task 2: Create Bitsight API Token

A Bitsight API token must be created and utilized within the JavaScript integration applications to connect to Bitsight. Below are the steps to create or locate the Bitsight API token.

1. Login to Bitsight Portal: <https://service.bitsighttech.com/>
2. Click on Gear  icon on top-right of screen
3. Click **Account** option

A screenshot of a computer

AI-generated content may be incorrect.

1. Scroll down to **Company API Token** section
2. Type a description in the text box under New Token.
   1. Suggested Description: Archer Bitsight VRM Integration
3. Ensure **All Companies** is selected or whatever scope your organization chooses to use.
4. Click the **Generate** button

A screenshot of a computer

AI-generated content may be incorrect.

1. Copy the **New Token Generated** text for use in the integration applications.

A screenshot of a computer

AI-generated content may be incorrect.

## Task 3: Configuring Integration between Archer and Bitsight

The integration applications must be configured correctly to successfully run.

This integration utilizes three JavaScript applications executed on a scheduled basis to perform the various tasks to pull data from Bitsight into Archer via API. This allows organizations utilizing SaaS, Hosted, or on-Prem to utilize the same solution.

Many organizations utilize special enterprise job scheduling software tools such as Tidal, ActiveBatch, BMC Control-M, etc. The steps outlined below demonstrate the configuration with Windows Task Scheduler, however many of the same concepts apply for other scheduling software.

**Important:** Ensure the server running the integrations applications can make outbound calls to the Internet if you are using a SaaS or Hosted Archer instance. You may need to work with your networking and/or data security teams to update the firewall rules for outbound calls over HTTPS (port 443) to both Bitsight and Archer.

**Steps:**

1. **Install Node.JS on Scheduling Server:**

No matter which job scheduling software you choose to implement, Node.JS must be installed to execute the applications. The latest version of Node.JS is recommended.

* + 1. Log into the server with administrator rights where you will run the JavaScript applications from programmatically.
    2. Download and install the node.js application from <http://nodejs.org>
       1. Choose all default options (or change as necessary)
       2. Regarding “Tools for Native Modules” you do NOT need to check the box to automatically install the necessary tools.

1. **Create Folder and Install Node Packages**
   * 1. Locate or create the folder/path where you want to run the JavaScript applications
        1. *Suggestion/Example: C:\Archer\BitsightVRM*
        2. *Tip: Avoid using spaces in your path/folder names for automated jobs*
     2. Install the required node packages with the Node Package Manager (npm)
        1. Open a “Node.js command prompt” from your Windows Start Menu
           1. *Tip: Pin the “Node.js command prompt” to your taskbar*
        2. Change directories to the path/folder created in the step above.
        3. Run the command: npm install @xmldom/xmldom
        4. Run the command: npm install axios
        5. Run the command: npm install xml2js
2. **Deploy the integration files and edit the config.js file**
   * 1. From the app-pack zip file, place the following files in the folder/path you created above:
        1. 100-CreateProfile.js
        2. 110-UpdateArcherTPP.js
        3. 120-UpdateArcherVendorFindings.js
        4. config.js
        5. nightly.bat
     2. Edit the config.js JavaScript file with your Archer URL, Archer Instance, Archer API Accounts, Archer paths, and Bitsight Token.
        1. Edit the **config.js** in any text editor (notepad, notepad++, etc.)
        2. Locate the params variable starting on line 6 and change the following settings to the appropriate setting for your company:
           1. archer\_username - The Archer user account you setup for the API above

Example: dfm\_BitsightVRMAPINightly

* + - * 1. archer\_password - Password for the accounts created above
        2. archer\_instanceName - Case sensitive name of your Archer Instance.

*Example: Dev*

*Note: SaaS/Hosted customers will have an instance number instead of text*

* + - * 1. archer\_webroot - Main URL of your Archer instance with a trailing slash.

*Example:* [*https://archer.mycompany.com/*](https://archer.mycompany.com/)

* + - * 1. Bitsight\_token - A valid Bitsight token is required to run the solution. See section above to create or locate your Bitsight Token.

*Example: “47460143ea9b6c6ahc5f873dbd5e5a1390adc2c5”*

* + - * 1. If your organization renamed the OOB “Third Party Profile” application to something else (example: Vendors), you must update the “archer\_ThirdPartyProfileApp” parameter with the new name of the application.

## Task 4: Optional: Configure the nightly.bat file

This task is not required unless you plan to monitor the output of the batch file execution and perform alerting with an internal system.

1. Edit the nightly.bat in any text editor (notepad, notepad++, etc.)
2. Locate and change the following settings to the appropriate setting for your company
   1. Change the Archer Instance Name on this line:
      1. set ArcherInstanceName=Dev
   2. *Note: This setting is informational for logging to help determine which instance is having issues should an error occur*
3. Save the .bat file

## Task 5: Setup Job Scheduling

Some organizations are required to use enterprise job schedulers such as Tidal, ActiveBatch, BMC Control-M, etc. Bitsight and Tutela cannot provide support for those tools, however the settings below for Windows Task Scheduler may help you with the necessary settings in your organization.

**Requirements:**

1. Windows Server
2. Administrator access to the Windows Server
3. A “service account” username and password that can run the job interactively
   1. Some organizations do not have an expiring password for these accounts while others rotate the passwords.
   2. Expiring passwords will need to be updated in Task Scheduler at the appropriate time.

**How to Set Up a Task Scheduler Task:**

1. Log into the Windows server with administrator rights where you will run the scripts from programmatically
2. Start the **Windows Task Scheduler** application on the server from the Start Menu
3. Create folders for Archer jobs
   1. Right-click **Task Scheduler Library** and click **New Folder**
   2. Type “Archer-BitsightVRM” and click **OK** button

**Creating the Nightly Job**

1. Right-click the “Archer-BitsightVRM” folder and click **Create Task…**
2. General Tab Settings:
   1. Name: Archer Bitsight VRM Nightly Jobs
   2. Description: This task launches the Bitsight VRM applications to process nightly jobs to replicate Bitsight VRM information in the Archer platform from the Bitsight API to enable our organization to effectively manage 3rd party security risk.
   3. Click the **Change User or Group…** button and set to a user account which has administrator or Logon as Batch privileges
      1. Note: You will likely need to setup an appropriate service account for this with a non-expiring password or a method to change the password and update the password in this task periodically.
   4. Change the radio button selection to **“Run whether user is logged on or not”**
   5. Set **Configure for** to current operating system
3. Triggers Tab Settings:
   1. Click **New…** button
   2. Begin the task: On a schedule
   3. Settings:
      1. Daily
      2. Start: Current Day at whatever time makes sense.
         1. Example: 4/1/2022 at 6:30am
         2. Based on Bitsight server processing, we would suggest starting this processing no earlier than 5am Eastern Time Zone (UTC -5).
      3. Recure every: 1 days
   4. Advanced Settings:
      1. Stop task if it runs longer than 8 hours: Checked
      2. Enabled: Checked
   5. Click **OK** button
4. Actions Tab Settings:
   1. Click **New…** button
   2. Action: **Start a program**
   3. Program/Script: [Full path to the batch file.]
      1. *Example: “C:\Archer\*BitsightVRM*\*nightly.bat”
   4. Start in (optional): [Full path of your batch file.]
      1. *Example: C:\Archer\*BitsightVRM*\*
   5. Click **OK** button
5. Conditions Tab Settings:
   1. Network: Start only if the following network connection is available:
      1. **Checked**
      2. Set dropdown to **Any Connection**
6. Settings Tab Settings:
   1. Allow task to be run on demand: **Checked**
   2. Stop the task if it runs longer than 8 hours: **Checked**
   3. If the running task does not end when requested, force it to stop: **Checked**
   4. If the task is already running, then the following rule applies: **Do not start a new instance**
7. Click the **OK** button to save your new task
8. Test the scheduled job
9. Right-click the scheduled job and click **Run**

## Task 6: Security and Hardening

### Bitsight Token

The Bitsight API Token used in the integration has the same privilege as the user who created the token. It is suggested to protect the API token as you would a username and password. While the API token cannot login to the Bitsight portal directly, any available functionality via the API could be used.

### Least Privilege Model

The Archer API security credentials used in this integration follow the least privilege access model by design. The Archer API account can only:

1. Read and update Third Party Profile records and values lists
2. Create, Read, and Update Bitsight VRM Findings records and values lists

### API Integration Code Security

Archer API security credentials and the Bitsight Token are accessible by anyone who can read the files in the integration code folder. It is suggested to restrict the access of the folder to the least amount of users as possible on a need to know basis.

# Chapter 5: Upgrading Bitsight VRM Integration

N/A - First release

# Chapter 6: Using Bitsight VRM Integration

## Additional Configuration

Many Archer customers continue to further configure/customize their Archer implementations to meet their organization’s unique needs and improve their risk posture.

These changes typically include:

1. Various verbiage/taxonomy changes
   1. Note: Caution is needed around integration points. Contact Tutela Solutions for assistance to ensure compatibility.
2. Security permissions with additional access roles, groups, record permissions and private fields
3. Customized email notifications upon certain events/triggers
4. New or updated dashboards and reports
5. Unique calculations of risk in Third Party Profile (TPP)
6. Additional linkage to other applications in Archer such as Incidents, Findings, Action Plans, and/or Exceptions, etc.
7. API integrations and/or Data Feeds to automate creation of records such as Incidents, Findings, etc. within Archer or integration outside of Archer to another system.

## Access Groups and Roles

No end-user roles were created for this integration. It is expected that your organization will have existing Third Party Risk Management roles that can be leveraged to access the Bitsight VRM data in Archer.

To setup the access, provide read access to the Bitsight VRM Findings questionnaire content. Here is the suggested rights for each role you want to provide access to:

A screenshot of a computer

AI-generated content may be incorrect.

*Note: Additional record permissions may need to be setup in TPP or Bitsight VRM Findings based on your organization’s security access model. Typically, the Relationship Manager field has access to the TPP record. Given Bitsight’s usage for managing risk, you are likely to use the Risk Analysts field. Please review the* ***Access Considerations*** *section below for additional implementation ideas to segment access further.*

## Bitsight Licensing Overview

The use of the Bitsight Archer integration will depend on your organization’s Bitsight VRM subscription and/or licensing model. Note that this process can utilize additional Bitsight VRM licenses for monitoring companies and needs to be managed.

## Bitsight Dashboard

No dashboards are included with this package. We encourage you to add the **Bitsight VRM Listing** report created in the setup instructions to an existing dashboard.

## High Level Process Overview

### Existing Bitsight VRM Customers (initial setup)

If you are an existing Bitsight VRM customer with a portfolio of companies/vendors in the Bitsight VRM Portal, the Nightly.bat job will update all your currently monitored companies/vendors from your portfolio into Archer’s TPP application when the Bitsight VRM Domain field is populated.

**NOTE: This only applies to companies in your VRM portfolio (Primary Domain) with a matching Bitsight VRM Domain in the TPP record…follow the steps below:**

**Steps:**

1. Populate the **Bitsight VRM Domain** field in all of the TPP records that you want to sync with the Primary Domain from the Bitsight VRM Portal.
2. Run the Nightly.bat script manually or wait for the scheduled job to run overnight.
3. View the **Bitsight VRM Listing** report in the Third Party Profile application to confirm the details of the VRM data were populated as expected.

### Monitor a New Vendor

The steps below outline the suggested process for organizations that want to create a new vendor to monitor in the Bitsight VRM Portal and load data back into Archer:

1. Create (or update) a vendor record in TPP adding the **Bitsight VRM Domain** field populated *(ex. bitsight.com)*
2. Overnight, the backend processes will automatically:
   1. Create the Bitsight VRM Vendor record to be monitored
   2. Update the TPP record with all the Bitsight VRM data available
   3. Create any findings in the Bitsight VRM Findings questionnaire

# Appendix A: Certification Environment

**Date Tested:** 4/15/2025

|  |  |  |
| --- | --- | --- |
| Product Name | Version Information | Operating System |
| Archer | 2024.09 | Windows |
| Bitsight VRM | 1.0 | N/A - SaaS |

# Appendix B: Access Considerations

You may want to consider adding inherited record permissions (IRP) from TPP to restrict access to specific Bitsight VRM Findings based on access from TPP.

You want to consider setting the Bitsight VRM fields in the TPP as private fields or using DDEs to restrict edit access to the data so only the Bitsight VRM API account can update the fields (except for the Bitsight VRM Domain field).

# Appendix C: Known Future Improvements

1. TBD.

# Appendix D: Frequently Asked Questions (FAQ)

**Q: Where can I find Bitsight’s knowledge base and glossary?**

A: Both the knowledge base and glossary can be found online here:

|  |  |
| --- | --- |
| Knowledge Base | <https://help.bitsighttech.com/hc/en-us/articles/115000320108-Bitsight-Knowledge-Base> |
| Bitsight Glossary | <https://help.bitsighttech.com/hc/en-us/sections/360002544953-Glossaries> |

**Q: Can I rename the Archer applications (Third Party Profile or Bitsight VRM Findings) for this solution?**

A: Yes, you can change the names of these fields in the config.js file.

Set archer\_ThirdPartyProfileApp to the name of your Third Party Profile application.

Set archer\_BitsightVRMFindings to the name of your Bitsight VRM Findings questionnaire.

**Q: Can I rename the Archer VRM field names in Third Party Profile or Bitsight VRM Findings?**

A: No, changing the names of the field names is not supported in this version since the integration code is expecting the field names to match exactly. This functionality may be considered in a future release.