Archer® Exchange

Archer® Suite

Version 6.7

Implementation Guide

December 2021

RiskRecon®—Own Enterprise Monitoring

Contact Information
RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

November 2020

Revised: December 2021

Table of Contents

Release Notes

What's New

The following table describes enhancements.

Date	Component	Description
December 2021	JavaScript	Re-Signed JavaScript file.
November 2020	Data Feeds, Applications	**Renamed Security Domains** The XSLT in the TPSRM_OE: Company 6.7 – JST data feed and the TPSRM_OE: Issues 6.7 – JST data feed was updated to account for the renaming of the following RiskRecon security domains: • Web Applications Security to Application Security • Data Loss to Breach Events • Threat Intelligence to System Reputation **Deprecated Security Domains** The XSLT has been updated to remove references to the Governance and Defensibility security domains to align with changes made by RiskRecon. **Note:** The Company and Vulnerability Scan Results applications were also updated due to the renamed and deprecated security domains.
November 2020	Values List	The values in the Security Domain values list in the Vulnerability Scan Results application were updated to reflect the renamed security domains.
November 2020	Applications	The Company and Vulnerability Scan Results applications were updated to add A-F letter grades implemented by RiskRecon. These letter grades now correspond with numerical risk rating scores for an overall grade.
October 2020	Data Feed, Company application	The Company application and the TPSRM_OE: Company 6.7 – JST data feed were updated to include the new Network Filtering security domain added by RiskRecon. For updates to the Company application, you must import the updated Archer 6.7 Own Enterprise Monitoring Install Package. For updates to the TPSRM_OE: Company 6.7 – JST data feed, you must import the updated TPSRM_OE: Company 6.7 – JST data feed. The install package and data feed files are contained in the RiskRecon Own Enterprise Monitoring Archer 6.7 Package ZIPfile, which is available on RSA Link.
September 2020	Data Feeds	The RiskRecon JavaScript file was updated for improved performance, severity filtering capability, and error handling for data feeds.

		For more information, see Configure the TPSRM_OE: Company 6.7 – JST Data Feed and Configure the TPSRM_OE: Issues 6.7 – JST Data Feed.
April 2020	Data Feeds	Added the Network Filtering Security Domain to transform in the TPSRM_OE: Issues 6.7 – JST data feed. This update accounts for a new Security Domain added by RiskRecon.

Fixed Issues

The following table describes fixed issues.

Date	Component	Description
September 2020	Data Feeds	For customers who have Archer configured to use HTTPS and have a self-signed SSL certificate or another form of non-perfected SSL certificate from a top tier Certificate Authority, data feeds were failing due to validation errors. To resolve this issue, the verifyCerts optional parameter was added to the TPSRM_OE: Company 6.7 – JST data feed and TPSRM_OE: Issues 6.7 – JST data feed. This parameter is set to 'true' by default, and you must set it to 'false' if you have Archer configured to use HTTPS and have a non-perfected SSL certificate in place.
April 2020	Data Feeds	The JavaScript code was updated to remove hardcoded GUIDs for the archerReportGUIDOE and archerKeyFieldGUIDOE parameters, which were causing the JavaScript to fail.
April 2020	Data Feeds	In a small number of instances, Unicode control characters were being returned in the JSON file retrieved from the RiskRecon API, which caused data feed failure. These characters were in the finding_data_value node and have been dropped by default. An additional parameter has been added to the JavaScript file to use if additional characters are ever introduced that cannot be ingested into Archer. For more information on this new parameter, see Configure the TPSRM_OE: Issues 6.7 – JST Data Feed.

Chapter 1: Overview of Own Enterprise Monitoring

About Own Enterprise Monitoring

The Archer Own Enterprise Monitoring integration, powered by RiskRecon, delivers transparent security measurements, analytics, and analyst-level insight to dramatically improve your Own Enterprise Monitoring risk management program. This integration provides organizations with visibility, insight and actionable intelligence into risk environments. Own Enterprise Monitoring discovers and analyzes each company's IT footprint using artificial intelligence (AI) to automatically measure the value of each asset. This enables analysts to quickly identify each specific system that poses the greatest risk, based on vulnerability severity and asset criticality.

Key Features and Benefits

- Receive an actionable view of security issues for each company.
- Pinpoint potential exposures and root causes for 50+ security criteria.
- Obtain on-demand assessments of any organization's security practices.
- Demonstrate risk control quality to regulators and standards bodies.
- Proactively identify common exposures throughout your web-facing presence.
- Gain objective insight into your security performance and IT landscape.
- Continuously monitor security performance.
- Optimize use of analysts' time and outside auditor resources.
- Allocate risk resources to where they are needed most, to focus on high-value, low-performing assets.

Important: This document refers to the RiskRecon Own Enterprise Monitoring integration. To take advantage of the functionality offered by this integration, you can use your RiskRecon license and complete the instructions in this guide to enable communication between Archer and your RiskRecon product. You do not need to also license Archer Third Party Security Risk Monitoring. However, you must have licenses for each of the prerequisite Archer use cases listed in this guideto make use of the functionality provided by this integration.

Requirements

Components	Requirement
Archer Solution	IT Security Risk Management
Archer Use Case	IT Security Vulnerabilities Program, Third Party Security Risk Monitoring or obtain a license from RiskRecon
Archer Applications	Company, Vulnerability Scan Results
Uses Custom Application	No
Requires On-Demand License	No

Applications

The following table describes the integration applications.

Application	Description
Vulnerability Scan Results	The Vulnerability Scan Results application stores the issues that result from every new record that is created from the vulnerability scanner such as Device Name, IP, owner, department, description, notes, recommendations, and much more. These records contain the technical recommendation for each scan result and allow for reporting on the total number of issues, regardless of which system detects it.
Company	The Company application stores general, financial, and compliance information at the company level. Combined with the Division and Business Unit applications, this application supports roll-up reporting of governance, risk, and compliance initiatives across the enterprise.

Access Roles and Record Permissions

The following table describes the integration access roles.

Access Roles	Permissions
ITSVP: Analysts	This role provides the appropriate access levels to Analysts within the IT Security Vulnerabilities Program use case to perform analysis and classify vulnerabilities accordingly.
ITSVP: Operations	This role provides the appropriate access levels to Operators within the the IT Security Vulnerabilities Program use case.
ITSVP: Executive Management	This role establishes the rights for Executive Management within the IT Security Vulnerabilities Program use case. Users with this role are provided with read access to the IT Security Vulnerabilities Program applications.
ITSVP: Business Management	This role provides access levels to the appropriate line of business within the IT Security Vulnerabilities Program use case.
ITSVP: Admin	This role serves as the administrator for the IT Security Vulnerabilities Program use case, providing create, read, update, and delete access rights.
ITSVP: Read Only	This role provides users with read-only access to ITSVP applications.

Dashboards

The following table describes the integration dashboard.

Dashboard	Description
Own Enterprise Monitoring	The Own Enterprise Monitoring dashboard provides a snapshot of your current footprint including overall and domain scoring, heat map of all open issues, ticket status, and any unassigned issues.

Data Feeds

The following table describes the integration data feeds.

Application	Description
TPSRM_OE: Company 6.7 – JST	The TPSRM_OE: Company 6.7 – JST data feed is a JavaScript Transporter feed that imports overall and domain-specific scores from Third Party Security Risk Monitoring. The data feed is preconfigured to update Company records when Third Party Security Risk Monitoring performs new scans. If you want to add additional security domain scores in the future, you may adjust the XSLT as needed.
TPSRM_OE: Issues 6.7 – JST	The TPSRM_OE: Issues 6.7 – JST data feed is a JavaScript Transporter feed that imports issues to the Vulnerability Scan Results application. The data feed is preconfigured to create new records when no match is found against the preconfigured data feed key, and to update records when Third Party Security Risk Monitoring creates, closes, or updates any issues. If you want to change the preconfigured data feed key, you may do so in the provided XSLT.

Chapter 2: Configuring Own Enterprise Monitoring

Before You Begin

This section provides instructions for configuring the RiskRecon - Own Enterprise Monitoring integration with the Archer Platform. This document is not intended to suggest optimum installations or configurations.

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

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.

Prior to version 6.7, customers were required to manually create fields in the Vulnerability Scan Results and Company applications that are unique to this integration. If you are installing or upgrading to 6.7 or later, you can automatically get these updates in the RiskRecon Own Enterprise Monitoring Archer 6.7 Package.

For this integration, you must download and install the RiskRecon Own Enterprise Monitoring Archer 6.7 Package.zip file from RSA Link.

Install the Integration Package

The following tasks detail how to import and install 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. It is strongly recommended to back up the instance database before installing a package. This process enables a full restoration if necessary.

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

Task 2: Import the Package

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

The package file is displayed in the Available Packages section and is ready for installation.

Task 3: Map Objects in the Package

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

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

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

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

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

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

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

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

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

    Note: To undo mapping settings for any individual object, click in the Actions column. When all objects are mapped, the icon is displayed in the tab title. The icon is displayed next to the object to indicate that the object will not be mapped.
5. Verify that all other objects are mapped correctly.
6. (Optional) To save your mapping settings so that you can resume working later, see "Exporting and Importing Mapping Settings" in the Archer Online Documentation.
7. Once you have reviewed and mapped all objects, click .
8. Select "I understand the implications of performing this operation," and then click OK.
   The Advanced Package Mapping process updates the system IDs of the objects in the target instance as defined on the Advanced Package Mapping page. When the mapping is complete, the Import and Install Packages page is displayed.

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

Task 4: Install the Package

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

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, do the following:
    a. Locate the package file that you want to install.
    b. In the Actions column, click  .
3. In the Selected Components section, select the components of the package that you wantto install.
    Note: Items in the package that do not match an existing item in the target instance are selectedby default.
4. Click Lookup.
5. For each component section, do the following:
    Note: To move on to another component section, click Continue or select a component sectionin the Jump To drop-down menu.
    a. In the Install Method drop-down menu, select an install method for each selected component.
        Note: If you have any existing components that you do not want to modify, selectCreate New Only. You may have to modify those components after installing the package to use the changes made by the package.
    b. In the Install Option drop-down menu, select an install option for each selected component.
        Note: If you have any custom fields or formatting in a component that you do not wantto lose, select Do not Override Layout. You may have to modify the layout after installing the package to use the changes made by the package.
6. Click OK.
7. To deactivate target fields and data-driven events that are not in the package, in the Post-Install Actions section, select the Deactivate target fields and data-driven events that are not in the package checkbox. To rename the deactivated target fields and data-driven events with a user-defined prefix, select the Apply a prefix to all deactivated objects checkbox, and enter a prefix. This can help you identify any fields or data-driven events that you may want to review for cleanup post-install.
8. Click Install.
9. Click OK.

Task 5: Review the Package Installation Log

1. Go to the Install Packages page.
2. Click the Package Installation Log tab.
3. Click the package that you want to view.

4. In the Package Installation Log page, in the Object Details section, click View All Errors.
   For a list of packaging installation log messages and remediation information for common messages, see "Package Installation Log Messages" in the Archer Online Documentation.

Obtain the Security Risk Monitoring IDs from Third Party Security RiskMonitoring

You must obtain the Security Risk Monitoring ID for each Company you want to track from Third Party Security Risk Monitoring prior to importing and running the data feeds. To obtain the Security Risk Monitoring ID, perform the following steps:

1. Log in to Third Party Security Risk Monitoring.
2. In the search bar at the top of the screen, enter the name of the company for which you want to obtain the Security Risk Monitoring ID.
3. Go to the Company Profile tab.
4. In the Assessment Configuration section, locate and copy the TOE ID value.
5. Save the TOE ID for later use.
6. Repeat steps 2-5 for each company you want to track.
   The Security Risk Monitoring ID (TOE ID) is inserted in Archer. See step 5 of Insert the Security Risk Monitoring ID (TOE ID) from Third Party Security Risk Monitoring.

Obtain the API Key from Archer Third Party Security Risk Monitoring

You must obtain an API key from Third Party Security Risk Monitoring prior to configuring the data feeds. To obtain a key, perform the following steps:

1. Log in to Third Party Security Risk Monitoring.
2. Go to My Account → System Administration.
3. Locate the account for which you want to obtain an API key and click Manage.
4. Select the API Keys tab under the System Administration section.
5. Click New API Key.
6. Enter a description for the API key.
7. Select a key expiration date.
8. Click Create API Key.
9. Click the clipboard located on the left side of the user account to copy the key to your clipboard, and then save it for later use.
   This API key is used when defining custom parameters for the TPSRM_OE: Company 6.7 – JST and the TPSRM OE: Issues – JST data feeds.

Insert the Security Risk Monitoring ID (TOE ID) from Third Party Security Risk Monitoring

Once you have obtained the Security Risk Monitoring ID (TOE ID) for each company from Third Party Security Risk Monitoring, you must insert it in each corresponding Company record before you importand run the data feeds. To insert the Security Risk Monitoring ID (TOE ID) in Archer, perform the following steps:

1. Open Archer.
2. Go to the Company page.
   a. From the menu bar, select IT Security Risk Management.

b. Under Solutions, select IT Asset Catalog.
c. Under Applications, select Company.

3. Select the Company for which you obtained the Security Risk Monitoring ID.
4. Click Edit.
5. In the General Information tab, insert the Security Risk Monitoring ID (TOE ID) in the Security Risk Monitoring ID field that you saved in step 5 of Obtain the Security Risk Monitoring IDs from Third Party Security Risk Monitoring.
6. Click Save and Close.
7. Repeat steps 2-6 for each Company.

Configure the JavaScript Transporter Settings

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

1. Open the Archer Control Panel.
2. Go to Instance Management and select All Instances.
3. Select the instance.
4. On the General tab, go to the JavaScript Transporter section.
5. In the Max Memory Limit field, set the value to 2048 MB (2 GB).
6. In the Script Timeout field, set the value to 120 minutes (2 hours).
7. Require Signature is enabled by default on install. Signed Certificate Thumbprints are required for all Hosted clients.
    a. In the Signing Certificate Thumbprints section, add a thumbprint for each digitally signed JavaScript file.
        i. Double-click an empty cell in the Signing Certificate Thumbprints section.
        ii. Enter the digital thumbprint of the trusted certificate used to sign the JavaScript file.

        Note: For more information on how to obtain digital thumbprints, see Digital Thumbprints.
        Important: If you enable Require Signature and do not specify thumbprints, JavaScript files will not be accepted by the system.
8. On the toolbar, click Save.

Digital Thumbprints

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

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

Archer Technologies LLC Certificate in the Trusted Root CA Store

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

1. On the JavaScript file, right-click and select Properties.
    a. Click the Digital Signatures tab.

b. From the Signature List window, select Archer Technologies LLC.
c. Click the Details button.
d. Click View Certificate.
e. Click Install Certificate.
f. Select Local Machine.
g. Click Next.
h. Select Place all certificates in the following store and click Browse.
    i. Select Trusted Root Certification Authorities and click OK.
    ii. Click Next.
    iii. Click Finish.

2. Upon successful import, click OK.

Obtain a Certificate Thumbprint

1. On the Web Server and Services Server machines, open the Manage Computer Certificates program.
    a. Launch "certmgr" from the Start menu.
    b. Navigate to Certificates – Local Computer > Trusted Root Certification Authorities > Certificates.
2. Verify that the certificate is trusted.
    a. Double-click the Archer Technologies LLC certificate.
    b. In the Certificate window, click the Certification Path tab.
    c. Ensure that the Certificate Status windows displays the following message: "This certificate is OK."
    Note: If the Certificate Status windows displays something different, follow the on-screen instructions.
3. Obtain the trusted certificate thumbprint.
    a. In the Certificate window, click the Details tab.
    b. Scroll to and select the Thumbprint field.
    The certificate's digital thumbprint appears in the window.
    c. Copy the thumbprint.
    Note: For information on adding digital thumbprints, see Step 7a of Configure the JavaScript Transporter Settings regarding where thumbprint is relevant.

Set up Third Party Security Risk Monitoring: Own Enterprise Monitoring Data Feeds

The Own Enterprise Monitoring integration contains two data feeds:

- TPSRM_OE: Company 6.7 – JST.dfx5
- TPSRM_OE: Issues 6.7 – JST.dx5

Import the TPSRM_OE: Company 6.7 – JST Data Feed

1. Log in to Archer.

2. Go to the Manage Data Feeds page:
    a. From the menu bar, click  .
    b. Under Integration, click Data Feeds.
3. In the Manage Data Feeds section, click Import.
4. Locate and select the TPSRM_OE: Company 6.7 – JST.dfx5 data feed file.
5. Verify settings in the General tab.
    a. In the General Information section, set the Status field to Active.
    b. In the Feed Information section, confirm that the Target field is set to Company.
6. Click the Transport tab.
7. In the Transport section, in the Transport Method field, select JavaScript Transporter.
8. In the Transport Configuration section, click Upload.
    a. Locate and select the TPSRM_6.6_v1.js JavaScript file.
9. In the Custom Parameters section, enter the following key values:

Key	Value
apiKey	[insert API Key from Third Party Security Risk Monitoring]
archerUrl	[insert the URL of your Archer instance]
archerInstance	[insert the name of your Archer instance]
archerUser	[insert user account name that has read access to all Company records]
archerPass	[insert password for the archerUser account name]
ownEnterprise	True
archerReportGUIDOE	[insert the report GUID for "Own Enterprise – Companies to Track"]
archerKeyFieldGUIDOE	[insert the field GUID for "Security Risk Monitoring ID" from the Company application]
vendorEndpoints	Enter one or more of the following endpoints: • hostEndpoint • descEndpoint • industryEndpoint • subEndpoint By default, this value is set to descEndpoint, industryEndpoint, subEndpoint.

10. The following additional parameters are valid options for the Custom Parameters section:

Key	Type	Value
proxy	Protected	[insert the URL of the proxy server] **Note:** This key should only be entered if you use a proxy server. If you are an Archer Hosted (SaaS) customer, this key is required, and you must contact your Professional Services representative to configure this parameter.
requestsPerMin	N/A	[Upper threshold of outgoing requests per minute. This value is pre-populated.]

concurrenyLimit	N/A	[Max number of in-flight requests at any given time. This value is pre-populated.]
maxRetry	N/A	[Max number of retries per individual requests. This value is pre-populated.
archerReportLimit	N/A	[Max number of vendors for which you want to retrieve data. This value is pre-populated and set to 1000 by default.]
verifyCerts	N/A	[true] or [false] By default, this value is set to true. If you have configured Archer to use HTTPS, and the SSL certificate is self- signed or is another form of non-perfected SSL certificatefrom a top-tier Certificate Authority, you must set this value to false.

11. Click Save.

Import the TPSRM_OE: Issues 6.7 – JST Data Feed

1. Log in to Archer.
2. Go to the Manage Data Feeds page:
    a. From the menu bar, click  .
    b. Under Integration, click Data Feeds.
3. In the Manage Data Feeds section, click Import.
4. Locate and select the TPSRM_OE: Issues 6.7 – JST.dfx5 data feed file.
5. Verify settings in the General tab.
    a. In the General Information section, set the Status field to Active.
    b. In the Feed Information section, confirm that the Target field is set to Vulnerability Scan Results.
6. Click the Transport tab.
7. In the Transport section, in the Transport Method field, select JavaScript Transporter.
8. In the Transport Configuration section, click Upload.
    a. Locate and select the TPSRM_6.6_v1.js JavaScript file.
9. In the Custom Parameters section, enter the following key values:

Key	Value
apiKey	[insert API Key from Third Party Security Risk Monitoring]
minimumSeverity	[severity[]=severitylevel] You must specify each severity level that you want to filter. The following severity levels are available: • Info • Low • Medium • High • Critical Examples:

	• If you want to retrieve critical and high issues, enter the following value: severity[]=critical&severity[]=high • If you only want to retrieve medium issues, enter the following value: severity[]=medium • If you want to retrieve all severity issues, enter the following value: severity[]=info&severity[]=low&severity[]=medium&severity[]=high&severity[]=critical
archerUrl	[insert the URL of your Archer instance]
archerInstance	[insert the name of your Archer instance]
archerUser	[insert user account name that has read access to all Third Party Profile records] **Note:** You can add this user to the Third Party: Read Only group for access.
archerPass	[insert password for the archerUser account name]
ownEnterprise	True
archerReportGUIDOE	[insert the report GUID for "Own Enterprise – Companies to Track"]
archerKeyFieldGUIDOE	[insert the field GUID for "Security Risk Monitoring ID" from the Company application]

10. The following additional parameters are valid options for the Custom Parameters section:

Key	Type	Value
proxy	Protected	[insert the URL of the proxy server] **Note:** This key should only be entered if you use a proxy server. If you are an Archer Hosted (SaaS) customer,this key is required, and you must contact your Professional Services representative to configure this parameter.
issuesDataToRemove	Plain Text	[insert the node to be dropped by the JavaScript file] **Note**: This parameter must match the exact spelling and casing of the JSON node. In a small number of instances, Unicode control characters were being returned in the JSON file retrieved from the RiskRecon API, which caused data feed failure. These characters were located in the finding_data_value node and have been dropped by default. This additional parameter has been added to the JavaScript file to use if additional characters are ever introduced that cannot be ingested into Archer.

requestsPerMin	N/A	[Upper threshold of outgoing requests per minute. This value is pre-populated.]
concurrencyLimit	N/A	[Max number of in-flight requests at any given time. This value is pre-populated.]
maxRetry	N/A	[Max number of retries per individual requests. This value is pre-populated.]
archerReportLimit	N/A	[Max number of vendors for which you want to retrieve data. This value is pre-populated and set to 1000 by default.]
verifyCerts	N/A	[true] or [false] By default, this value is set to true. If you have configured Archer to use HTTPS, and the SSL certificate is self- signed or is another form of non-perfected SSL certificate from a top tier Certificate Authority, you must set this valueto false.

11. Click Save.

Schedule Data Feeds

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

As you schedule your data feed, the Data Feed Manager validates the information. If any information is invalid, an error message displays. You can save the data feed and correct the errors later; but the data feed does not process until you make corrections.

1. Go to the Schedule tab of the data feed that you want to modify.
    a. From the menu bar, click  .
    b. Under Integration, click Data Feeds.
    c. Select the data feed.
    d. Click the Schedule tab.
2. Go to the Recurrences section and complete frequency, start and stop times, and time zone. The following table describes the fields in the Recurrences section.

Field	Description
Frequency	Specifies the interval in which the data feed runs, for example, Minutely, Hourly, Daily, Weekly, Monthly, or Reference. • Minutely. Runs the data feed by the interval set. For example, if you specify 45 in the Every list, the data feed executes every 45 minutes. • Hourly. Runs the data feed by the interval set, for example, every hour (1), every other hour (2) and so forth.

	• Daily. Runs the data feed by the interval set, for example, every day (1), every other day (2) and, so forth. • Weekly. Runs the data feed based on a specified day of the week, for example, every Monday of the first week (1), every other Monday (2), and so forth. • Monthly. Runs the data feed based on a specified week of the month, for example, 1st, 2nd, 3rd, 4th, or Last. • Recurrence. Runs a specified data feed as runs before the current one. This option indicates to the Data Feed Service that this data feed starts as soon as the referenced data feed completes successfully. For example, you can select to have a Threats data feed run immediately after your Assets data feed finishes. From the Reference Feed list, select after which existing data feed the current data feed starts. A reference data feed will not run when immediately running a data feed. The Run Data Feed Now option only runs the current data feed
Every	Specifies the interval of the frequency in which the data feed runs.
Start Time	Specifies the time the data feed starts running.
Start Date	Specifies the date on which the data feed schedule begins.
Time Zone	Specifies the time zone in of the server that runs the data feed.

3. (Optional) To override the data feed schedule and immediately run your data feed, in the Run Data Feed Now section, click Start.
4. Click Save.

Editing the XSLT

XSLT is a language used for transforming the structure or format of XML documents. XSLT is used to manipulate XML documents into a format that can be properly ingested into Archer. When Own Enterprise Monitoring, powered by RiskRecon, adds new security domains to monitor, you must modify the XSLT contained in the TPSRM_OE: Company 6.7 – JST and TPSRM_OE: Issues 6.7 – JST data feeds to account for the changes.

Modify the XSLT in the TPSRM_OE: Company 6.7 – JST Data Feed

> **Important**: RSA recommends using an API development environment to make an API call to RiskRecon to determine the naming convention used for the new security domain and how it is referenced in the Rating and Web Directory nodes.

1. Log in to your instance.
2. Go to the Manage Data Feeds page.
    a. From the menu bar, click .
    b. Under Integration, click Data Feeds.
3. Locate and select the TPSRM_OE: Company 6.7 – JST data feed.
4. Click the Navigation tab.
5. Go to the XML File Definition section and do the following:
    a. Press CTRL+A to select all the text in the XSLT.
    b. Press CTRL+C to copy all the text in the XSLT.
6. Open an external text editor.
7. Paste the text in the external text editor.
8. Save the file with a new file name to prevent overwriting the original XSLT.
9. To add a new security domain rating, you must identify the name of the new domain that is being delivered from Third Party Security Risk Monitoring. This new domain name is typically in the format of <{domain_name}_rating>.
10. Once you have the name that is being passed back, create a new tag configuration within the XSLT. The format is provided in the following example:

```
<{domain name}_Rating>
        <xsl:value-of select="{domain_name}_rating"/>
</{domain name}_Rating>
```

11. Save the file in the external text editor.
12. Press CTRL+A to select all the text.
13. Press CTRL+C to copy all the text.
14. Reopen the Archer window that you had open in step 5.
15. In the XML File Definition section, press CTRL+A to select the original XSLT.
16. To overwrite the original XSLT, press CTRL+V to paste the modified XSLT.
17. Click Save.

Modify the XSLT in the TPSRM_OE: Issues 6.7 – JST Data Feed

The XSLT contained in the TPSRM_OE: Issues 6.7 – JST data feed is used to modify the format of the XML that contains the issues linked to each Security Criteria and Security Domain. This XLST also converts the data contained in the securityDomain node into a name appropriate for Archer.

> **Important:** RSA recommends using an API development environment to make an API call to RiskRecon to determine the naming convention used for the new security domain and how it is referenced in the Rating and Web Directory nodes.

1. Log in to your instance.
2. Go to the Manage Data Feeds page.

a. From the menu bar, click .
b. Under Integration, click Data Feeds.

3. Locate and select the TPSRM_OE: Issues 6.7 – JST.dfx5 data feed file.
4. Click the Navigation tab.
5. Go to the XML File Definition section and do the following:
   a. Press CTRL+A to select all the text in the XSLT.
   b. Press CTRL+C to copy all the text in the XSLT.
6. Open an external text editor.
7. Paste the text in an external text editor.
8. Save the file with a new file name to prevent overwriting the original XSLT.
9. Navigate to the beginning of the <xsl:choose> loop contained on line 255 of the out-of-the-box XSLT.

   Note: Within this loop, Archer tests the value returned in the securityDomain node. Depending on that value, Archer assigns specific text to the RiskReconDomain variable.
10. Copy the following three lines of code that begin on line 256 and end on line 258:

```
<xsl:when test="$securityDomain='software_patching'">
        <xsl:value-of select="'Software Patching'"/>
</xsl:when>
```

11. Paste the three lines of code from step 10 after the </xsl:when> tag on line 294 and beforethe </xsl:choose> tag on line 295.
12. In the lines of code you pasted in step 11, change the text after "$securityDomain= to incorporate the new security domain. You must use all lowercase letters with an underscore (_) between words.
    - For example, if the new security domain was titled Network Filtering, makethe following revision:

      <xsl:when test="$securityDomain='network_filtering'">

13. Change the text after the <xsl:value-of select="' text to incorporate the new security domain.
    - For example, if the new security domain was titled Network Filtering, makethe following revision:

      <xsl:value-of select="'Network Filtering'"/>

14. After making these changes, the new lines of text should look like the following text:

```
<xsl:when test="$securityDomain='network_filtering'">
        <xsl:value-of select="'Network Filtering'"/>
</xsl:when>
```

15. Save the file in the external text editor.
16. Press CTRL+A to select all the text.
17. Press CTRL+C to copy all the text.
18. Reopen the Archer window that you had open in step 5.
19. In the XML File Definition section, press CTRL+A to select the original XSLT.
20. To overwrite the original XSLT, press CTRL+V to paste the modified XSLT.
21. Click Save.

Chapter 3: Using Own Enterprise Monitoring

You can use the Own Enterprise Monitoring use case to track the risk ratings for your Companies and manage scan results.

For more information about using Own Enterprise Monitoring, see “Managing Scan Results” in the IT Security Vulnerabilities Program use case within the Archer Online Documentation.

Appendix A: Certification Environment

Date Tested: November 2020

Product Name	Version Information	Operating System
Archer	6.7	Virtual Appliance
RiskRecon	November 2020	SaaS