

# RSA<sup>®</sup> ARCHER<sup>®</sup> SUITE Implementation Guide

Axonius Cybersecurity Asset Management - RSA Archer Integration  
Release 6.5 P2



## 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 to [www.emc.com/legal/emc-corporation-trademarks.htm](http://www.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.

Copyright 2010-2019 Dell, Inc. or its subsidiaries. All Rights Reserved.  
May 2019

## Table of Contents

Chapter 1: Overview .....	4
About Axonius Cybersecurity Asset Management .....	4
Key Features and Benefits .....	4
Requirements.....	4
Integration Diagram.....	5
Chapter 2: Configure Axonius Cybersecurity Asset Management.....	6
Configure Axonius.....	6
Axonius Setup .....	6
Configure RSA Archer.....	7
Add Fields to the Devices Application.....	7
Configure the Data Feed .....	9
Configure the JavaScript Transporter Settings .....	9
Obtaining Digital Thumbprints.....	10
RSA Security LLC cert in the Trusted Root CA Store.....	10
Obtaining a Certificate Thumbprint .....	11
Setup the Axonius Devices Data Feed.....	11
Scheduling Data Feeds .....	13
Appendix A: Certification Environment .....	15

# Chapter 1: Overview

## About Axonius Cybersecurity Asset Management

The combination of the Internet of Things (IoT), Bring Your Own Device (BYOD), and cloud has changed our definition of access, and removed the line between work and home. Anything that can be connected will be, and we still expect IT and Security teams to manage and secure everything despite increasing fragmentation.

Axonius offers a cybersecurity asset management platform providing actionable visibility and security policy enforcement for all assets and users by aggregating existing business data from more than 100 management and security solutions.

To assess and control IT risks, organizations must have visibility into what could create risk. To accomplish this, risk owners and key stakeholders need the most comprehensive view of their organization's assets and how these entities support the company's mission. The Axonius Integration provides a single-system view of record to understand what devices are within their network, direct or indirect.

## Key Features and Benefits

Axonius provides RSA Archer and our customers with the ability to connect to more than 100 vendor solutions, including ServiceNow CMDB, Microsoft SCCM, Amazon AWS, Forescout, IBM BigFix, and many other leading endpoint security solutions. These vendor connections provide asset profile information to customers through one single connection. The Axonius Integration also provides RSA Archer the ability to access the most comprehensive list of assets to determine your role and the risk to your organization.

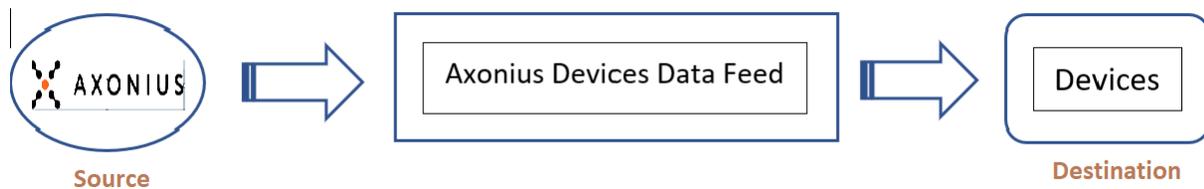
## Requirements

Components	Requirement
<b>RSA Archer Solution</b>	<ul style="list-style-type: none"> <li>• Audit Management</li> <li>• IT &amp; Security Risk Management</li> <li>• Regulatory &amp; Corporate Compliance Management</li> <li>• Third Party Governance</li> </ul>
<b>RSA Archer Use Case(s)</b>	<p>The following use cases can take advantage of the information provided by the Axonius integration:</p> <ul style="list-style-type: none"> <li>• RSA Archer Audit Engagements &amp; Workpapers 6.1</li> <li>• RSA Archer Third Party Governance 6.5</li> <li>• RSA Archer Business Continuity and Disaster Recovery Planning 6.5</li> <li>• RSA Archer IT Controls Assurance 6.5</li> <li>• RSA Archer IT Security Vulnerability Program 6.5</li> <li>• RSA Archer IT Risk Management 6.5</li> <li>• RSA Archer Cyber Incident &amp; Breach Response 6.5</li> <li>• RSA Archer PCI Management 6.5</li> <li>• RSA Archer Information Security Management System (ISMS) 6.5</li> <li>• RSA Archer Data Governance 6.5</li> </ul>

Components	Requirement
<b>RSA Archer Applications</b>	Leverages the Devices application
<b>Uses Custom Application</b>	No
<b>Requires On-Demand License</b>	No
<b>RSA Archer Requirements</b>	RSA Archer release 6.5 P2 or later
<b>Axonius Requirements</b>	Valid Axonius license is required

### Integration Diagram

The following diagram provides an overview of interaction between Axonius and the RSA Archer Axonius Integration offering.



The integration process follows this flow:

1. The RSA Archer data feed for the Axonius Integration pulls the data from the source: Axonius URL and imports the data into Target: Devices Application.
2. When the user logs into the Axonius URL, a list of all the devices/adapters available is visible.

## Chapter 2: Configure Axonius Cybersecurity Asset Management

This section provides instructions for configuring the Axonius Cybersecurity Asset Management offering with the RSA Archer Platform. This document is not intended to suggest optimum installations or configurations.

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

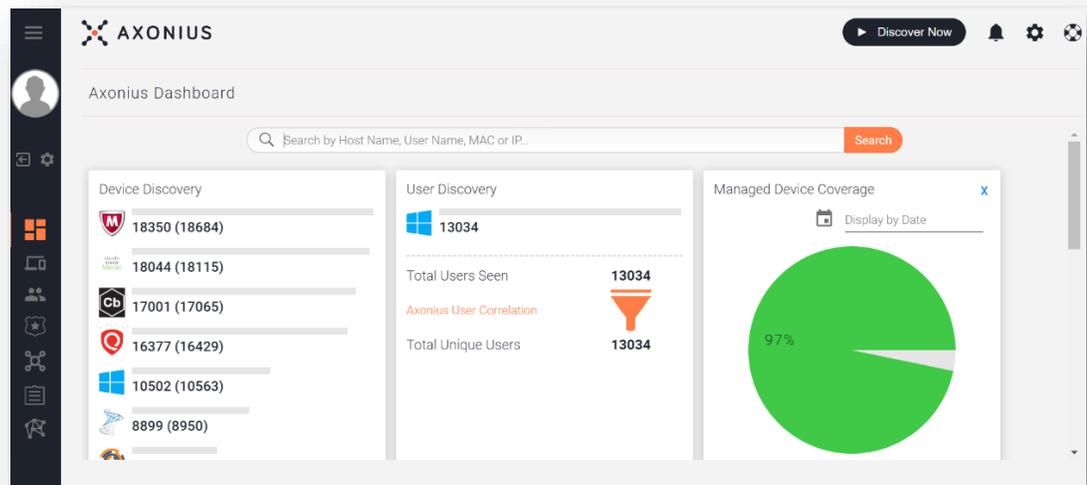
All Axonius components must be installed and working prior to the integration. Perform the necessary tests to confirm before proceeding.

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

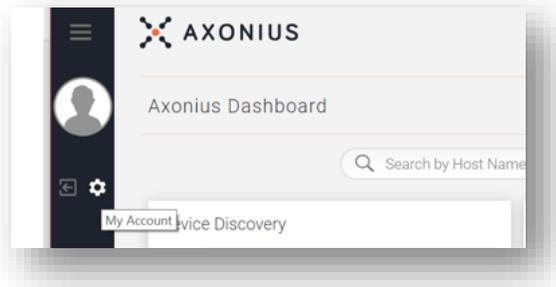
### Configure Axonius

#### Axonius Setup

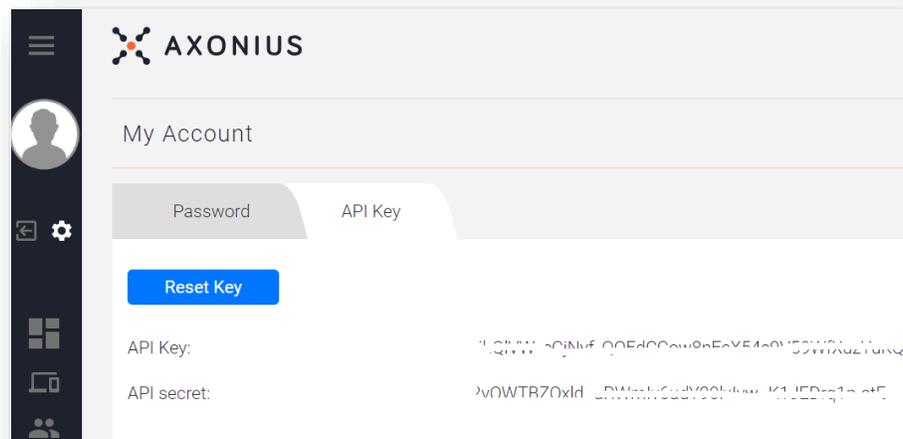
1. Log in to Axonius.



2. Go to “My Account”.



3. Generate the API-Key and Secret Key as shown below.



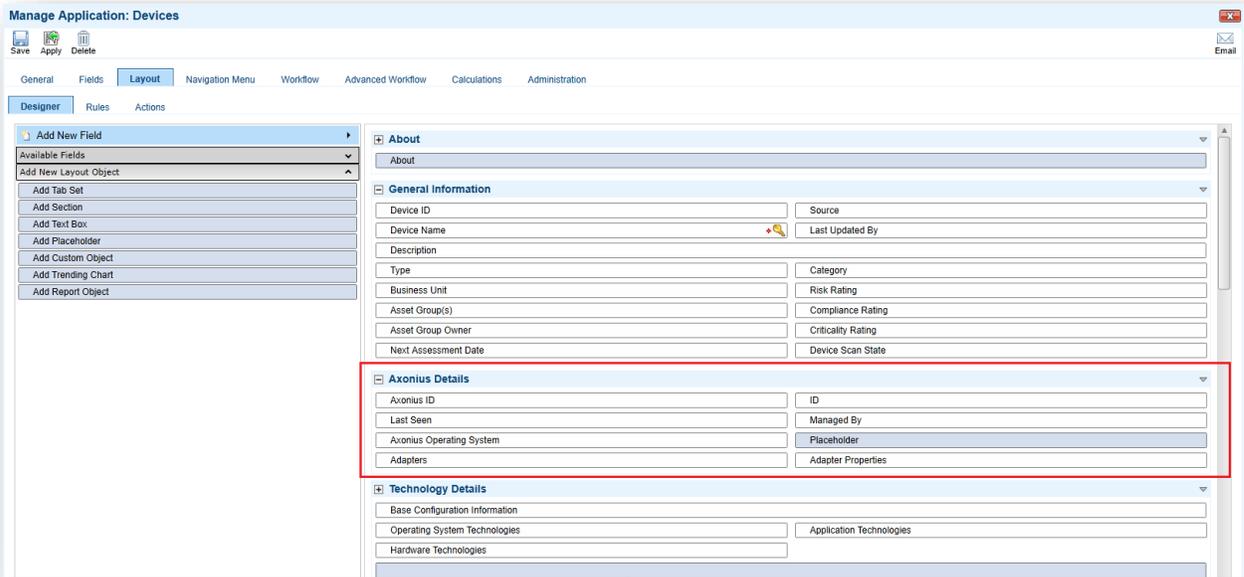
## Configure RSA Archer

Complete the following tasks to use the Devices application for the Axonius Integration.

### Add Fields to the Devices Application

1. Navigate to Applications by clicking the **Administration** and selecting **Applications** under the **Application Builder**.
2. Select the Devices Application -> Go to **Fields**. Add/Modify the fields below:
  - a. Source – Add a new value “Axonius” to the Values
  - b. Last Updated By – Add a new value “Axonius” to the Values  
**Note:** Both Source and Last Updated By fields use the same GVL “Enterprise: Device Sources”
  - c. Device Name – (No Modifications required)
  - d. Host Name – (No Modifications required)
  - e. Domain Name – (No Modifications required)
  - f. ID – Text field (New)
  - g. Last Seen – Date (New), Dropdown - Date and Time
  - h. Axonius Operating System – Values List Field (New), Dropdown [No Min., Max=1]

- i. Managed By – Values pop-up Values List field (New)
  - j. Location – (No Modifications required)
  - k. Adapter Properties – Values pop-up Values List field (New) [No Min, No Max]
  - l. Adapters – Values pop-up Values List field (New) [No Min, No Max]
  - m. Axonius ID –Text field
3. Go to **Layout**.
4. Add a new section named “Axonius Details”.
5. Add all the newly created fields to this section as shown in the screen shot below.



6. Click **Save**.

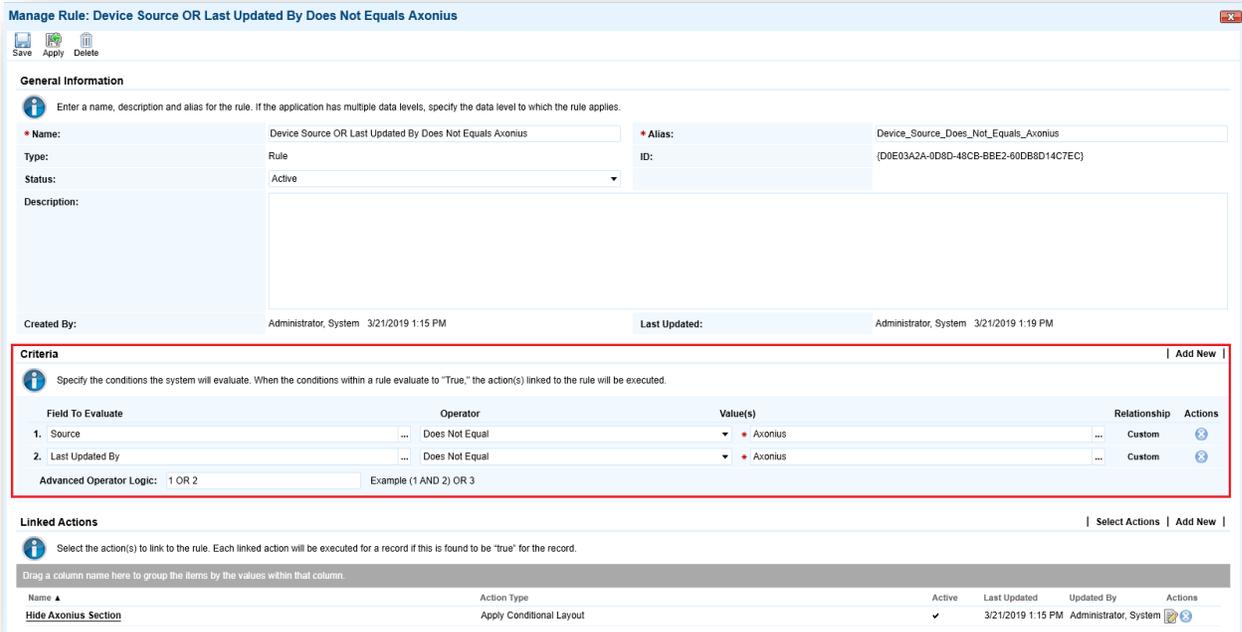
- Go to **Layout -> Rules**. Add a New Rule and Action.

**Rule:** Source **Does Not Equal** Axonius

Last Updated By **Does Not Equal** Axonius

**Action:** (Apply Conditional Layout) Hide Axonius Details Section

**Advanced Operator Logic:** 1 OR 2



## Configure the Data Feed

The following data feed is used as part of the Axonius Integration process:

Axonius Devices data feed is a JavaScript transporter data feed that retrieves data (Devices related data) from the Axonius URL and creates and updates the records in the RSA Archer Devices application.

**All data feeds must be configured.** After setting up the data feeds, you can schedule them to run **as needed per your organization’s requirements**. For more information on Scheduling data feeds, see the [Scheduling Data Feeds](#) section.

## Configure the JavaScript Transporter Settings

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

- On the General tab, go to the **JavaScript Transporter** section.
  - Open the **RSA Archer Control Panel**.
  - Go to **Instance Management** and select **All Instances**.

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

**Note:** For information on how to obtain digital thumbprints, see [Obtaining Digital Thumbprints](#).

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

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

### Obtaining Digital Thumbprints

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

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

### RSA Security LLC cert in the Trusted Root CA Store

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

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

## Obtaining a Certificate Thumbprint

1. In the RSA Archer Control Panel environment, open the Manage Computer Certificates program.
  - a. Click Start.
  - b. Type: certificate
  - c. From the search results, click **Manage Computer Certificates**.
2. Ensure that your trusted source certificates are in the **Certificates** sub-folder of the **Trust Root Certification Authorities** folder.
3. In the **Certificates** sub-folder, double-click the RSA Security LLC certificate that contains the thumbprint you want to obtain.
4. Verify that the certificate is trusted.
  - a. In the Certificate window, click the Certification Path tab.
  - b. Ensure that the Certificate Status windows displays the following message:  
THIS certificate is OK.

**Note:** If the Certificate Status windows displays something different, follow the on-screen instructions.

5. Obtain the trusted certificate thumbprint.
  - a. In the Certificate window, click the Details tab.
  - b. Select the Thumbprint field.  
The certificate's digital thumbprint appears in the window.

## Setup the Axonius Devices Data Feed

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

1. Go to the **Manage Data Feeds** page.
  - a. From the menu bar, click .
  - b. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click **Import**.
3. Locate and select the **Axonius Devices Data feed.dfx5** file.
4. Click Open.
5. In the **General Information** section, in the **Status** field, select **Active**.
6. Click the **Transport** tab.
7. In the **Transport Configuration** section, do the following:
  - a. Click Upload
  - b. From the Upload JavaScript File dialog, click **Add New**.
  - c. Locate and select the **axonius\_devices\_integration.js** file.
  - d. Click Open.

- e. From the **Upload JavaScript File** dialog, click **OK**.
8. In the Custom Parameters section, enter key values. The following table describes the value for each key in Custom Parameters.

Key	Value
<b>url</b>	Axonius URL
<b>api-secret</b>	[Valid value] Default = [empty]
<b>api-key</b>	[Valid value] Default = [empty]
<b>proxy</b>	[Valid value] Default = [empty] (Optional)

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

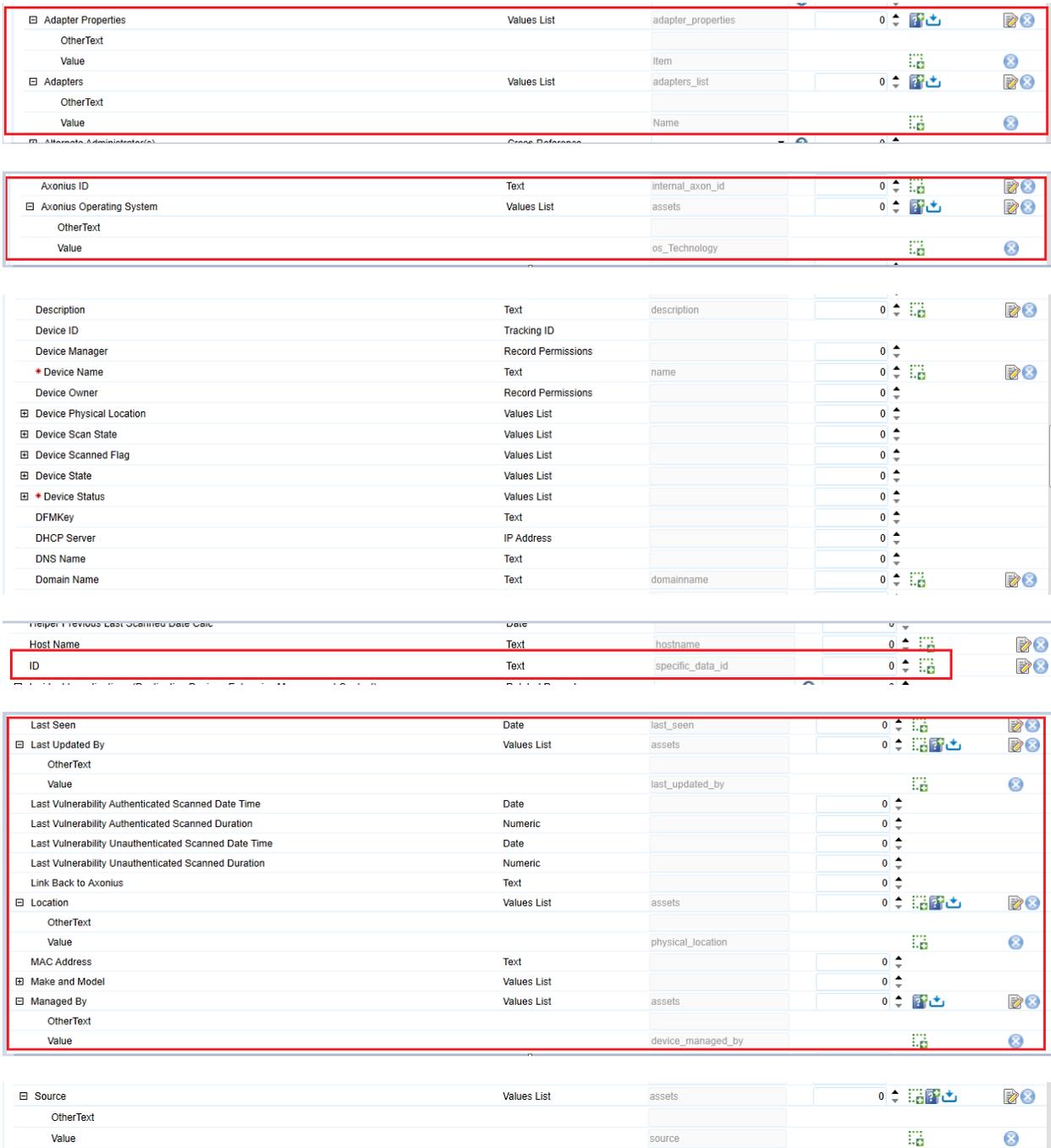
Key	Value
<b>verifyCerts</b>	[Valid value of true/false] Default = False

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

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

Source Field	Target Field
<b>Internal_axon_id</b>	Axonius ID
<b>specific_data_id</b>	ID
<b>last_seen</b>	Last seen
<b>adapter_properties</b>	Adapter Properties
<b>adapters_list</b>	Adapters
<b>device_managed_by</b>	Managed By
<b>os_technology</b>	Axonius Operating System

The screen shots below provide examples of these field mappings.



- In the Key Field Definitions Sub tab, add the “Axonius ID” as key field for Devices.

## Scheduling Data Feeds

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

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

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

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

Field	Description
<b>Frequency</b>	<p>Specifies the interval in which the data feed runs.</p> <ul style="list-style-type: none"> <li>• <b>By minute:</b> Runs the data feed by the minute interval set. For example, if you specify 45 in every list, the data feed executes every 45 minutes.</li> <li>• <b>Hourly:</b> Runs the data feed by the hourly interval set. For example, every hour (1), every other hour (2), and so forth.</li> <li>• <b>Daily:</b> Runs the data feed by the daily internal set. For example, every day (1), every other day (2), and so forth.</li> <li>• <b>Weekly:</b> 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.</li> <li>• <b>Monthly:</b> Runs the data feed based on a specified week of the month. For example, 1st, 2nd, 3rd, 4th, or Last.</li> <li>• <b>Reference:</b> Runs a specified data feed as runs before the current one. This option indicates to the Data Feed Service that this data feed starts as soon as the referenced data feed completes successfully. From the Reference Feed list, select after which existing data feed the current data feed starts. A reference data feed will not run when immediately running a data feed. The Data Feed Now option only runs the current data feed.</li> </ul>
<b>Every</b>	Specifies the interval of the frequency in which the data feed runs.
<b>Start Time</b>	Specifies the time the data feed begins running.
<b>Start Date</b>	Specifies the date on which the data feed schedule begins.
<b>Time Zone</b>	Specifies the time zone in of the server that runs the data feed.

5. Test the data feed to ensure that all device details from Axonius were imported into the Devices application. If testing fails, try verifying the data feed and re-run. If you experience multiple failures, please contact your RSA Partner.

## Appendix A: Certification Environment

**Date Tested:** May 2019

Product Name	Version Information	Operating System
RSA Archer Suite	Release 6.5 P2 and later	Virtual Appliance
Axonius	NA	NA