Archer® Exchange

Archer® Suite

6.9 SP1

Integration Guide

1.2

Axonius

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.

January 2021

Revised: January 2021

Table of Contents

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 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 Archer the ability to access the most comprehensive list of assets to determine your role and the risk to your organization.

Requirements

Components	Requirement
Archer Solution	• Audit Management • IT & Security Risk Management • Regulatory & Corporate Compliance Management • Third Party Governance
Archer Use Case(s)	The following use cases can take advantage of the information provided by the Axonius integration: • Archer Audit Engagements & Workpapers 6.1 and later • Archer Third Party Governance 6.5 and later • Archer Business Continuity and Disaster Recovery Planning 6.5 and later • Archer IT Controls Assurance 6.5 and later • Archer IT Security Vulnerability Program 6.5 and later • Archer IT Risk Management 6.5 and later • Archer Cyber Incident & Breach Response 6.5 and later • Archer PCI Management 6.5 and later • Archer Information Security Management System (ISMS) 6.5 and later • Archer Data Governance 6.5 and later

Components	Requirement
Archer Applications	Leverages the Devices application
Uses Custom Application	No
Requires On-Demand License	No
Archer Requirements	Archer release 6.5 P2 or later up to 6.9 SP1
Axonius Requirements	Valid Axonius license is required

Impacted Use Case(s)

Archer Use Case(s)
• **Archer Audit Engagements & Workpapers 6.1 and later** • **Archer Third Party Governance 6.5 and later** • **Archer Business Continuity and Disaster Recovery Planning 6.5 and later** • **Archer IT Controls Assurance 6.5 and later** • **Archer IT Security Vulnerability Program 6.5 and later** • **Archer IT Risk Management 6.5 and later** • **Archer Cyber Incident & Breach Response 6.5 and later** • **Archer PCI Management 6.5 and later** • **Archer Information Security Management System (ISMS) 6.5 and later** • **Archer Data Governance 6.5 and later**

Impacted Fields

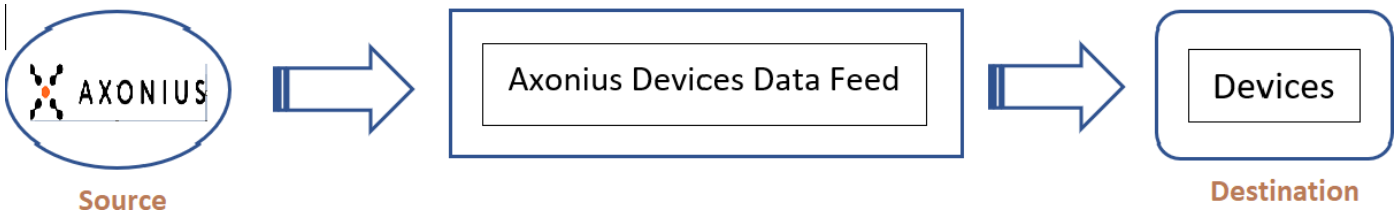
Archer Application	Archer Field	Axonius Field
Devices	**Axonius ID**	id
Devices	**Axonius Operating System**	os_technology
Devices	**Adapters**	adapters_list
Devices	**Adapter Properties**	adapters_properties
Devices	**Description**	description
Devices	**Device Unique Key**	DFMKey
Devices	**Domain Name**	domainname
Devices	**Host Name/Primary DNS Server Name**	hostname
Devices	**ID**	specific_data_id
Devices	**Last Updated By**	last_updated_by
Devices	**Last seen**	last_seen
Devices	**Managed By**	device_managed_by
Devices	**Device Name**	name_list/name
Devices	**Location**	physical_location
Devices	**Source**	source

Integration Diagram

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

The integration process follows this flow:

1. The 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 logins 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 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.

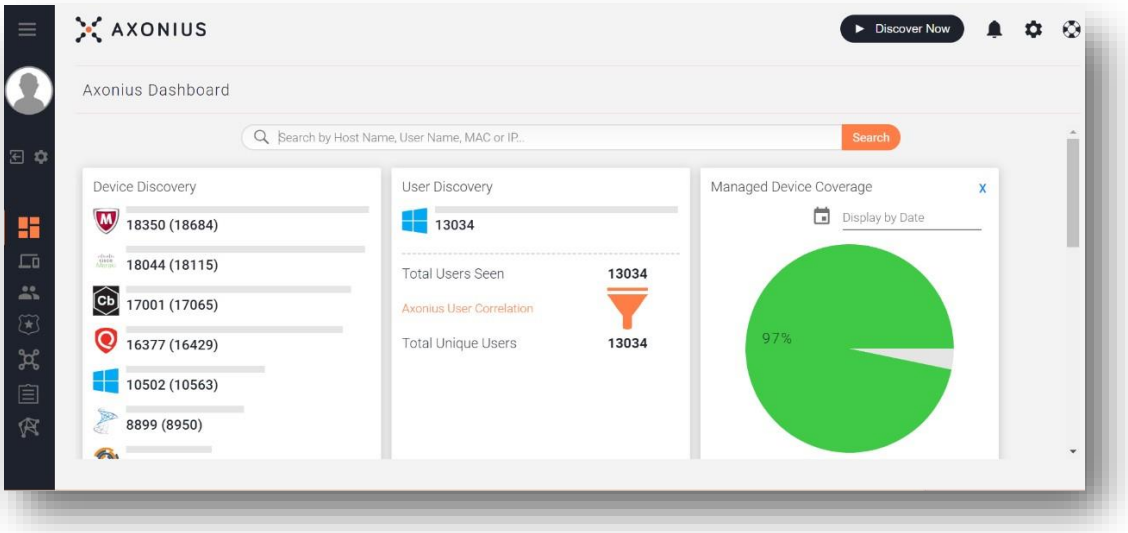
All Axonius components must be installed and working prior to the integration. Perform the necessary tests to confirm before proceeding.

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.

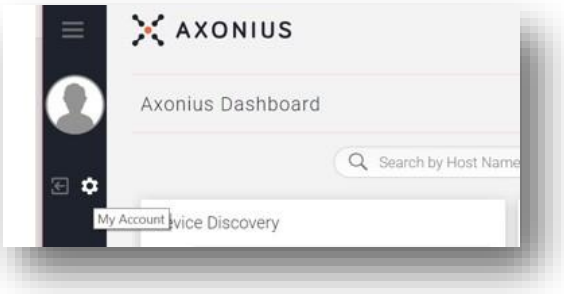
Configure Axonius

Axonius Setup

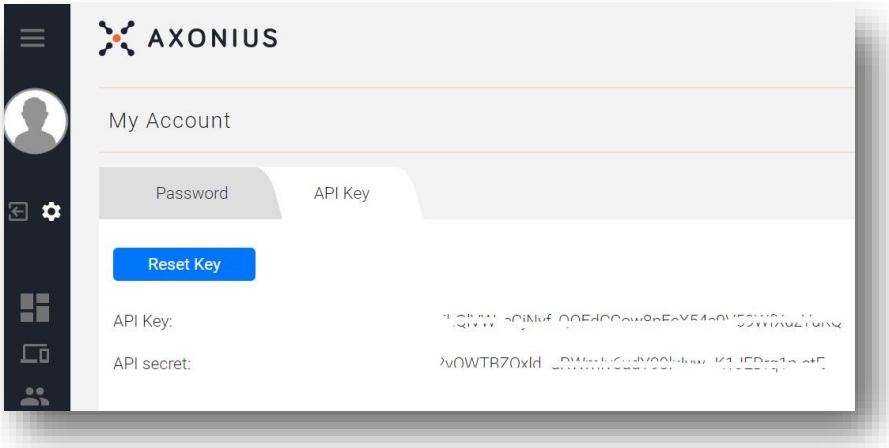
1. Log in to Axonius.



2. Go to “My Account”.



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

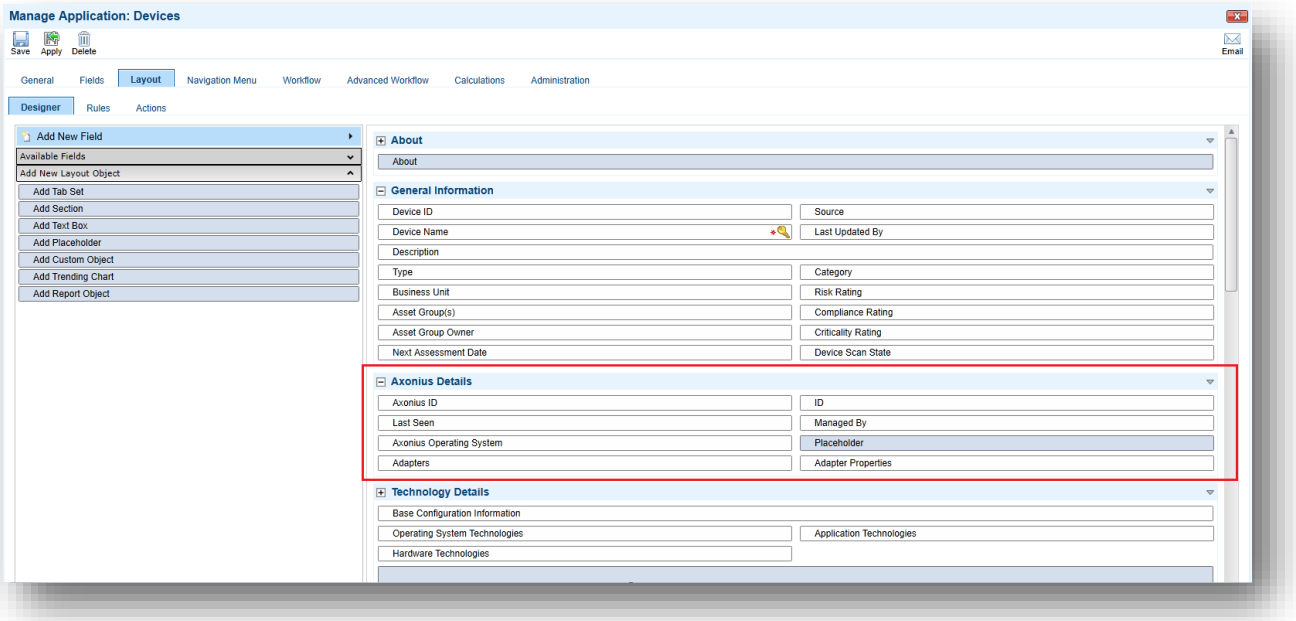


Configure Archer

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 – Text 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.**

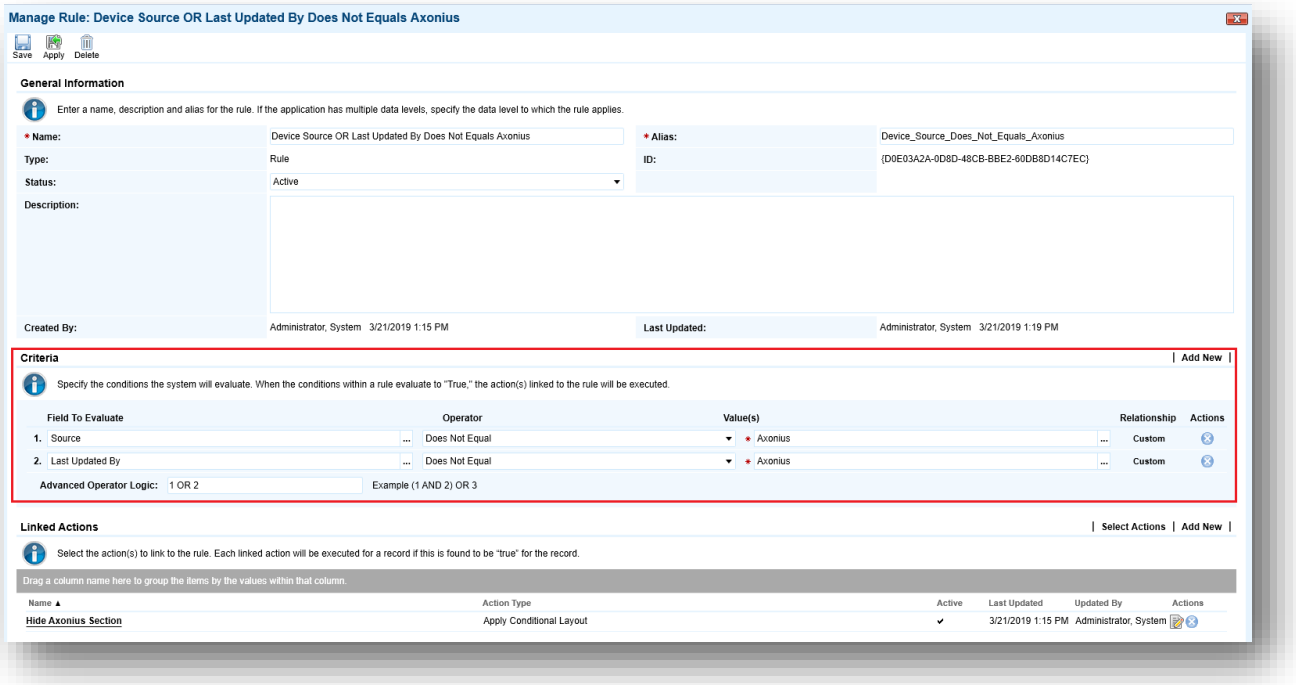
7. Go to **Layout** -> **Rules**. Add a New Rule and Action.

   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 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 Archer Control Panel.

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

c. Select the instance you want to use.
d. On the **General** tab, go to the **JavaScript Transporter** section.

2. In the **Max Memory Limit** field, set the value to 2048 MB (2 GB).
3. In the **Script Timeout** field, set the value to 120 minutes (2 hours).
4. (Optional) 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 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.

Axonius cert in the Trusted Root CA Store

Axonius 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 **Axonius Archer Integration** certificate.
   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 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 **Axonius Archer Integration** 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 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
url	Axonius URL
api-secret	[Valid value] Default = [empty]
api-key	[Valid value] Default = [empty]
Proxy	[Valid value] Default = [empty] (Optional)

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

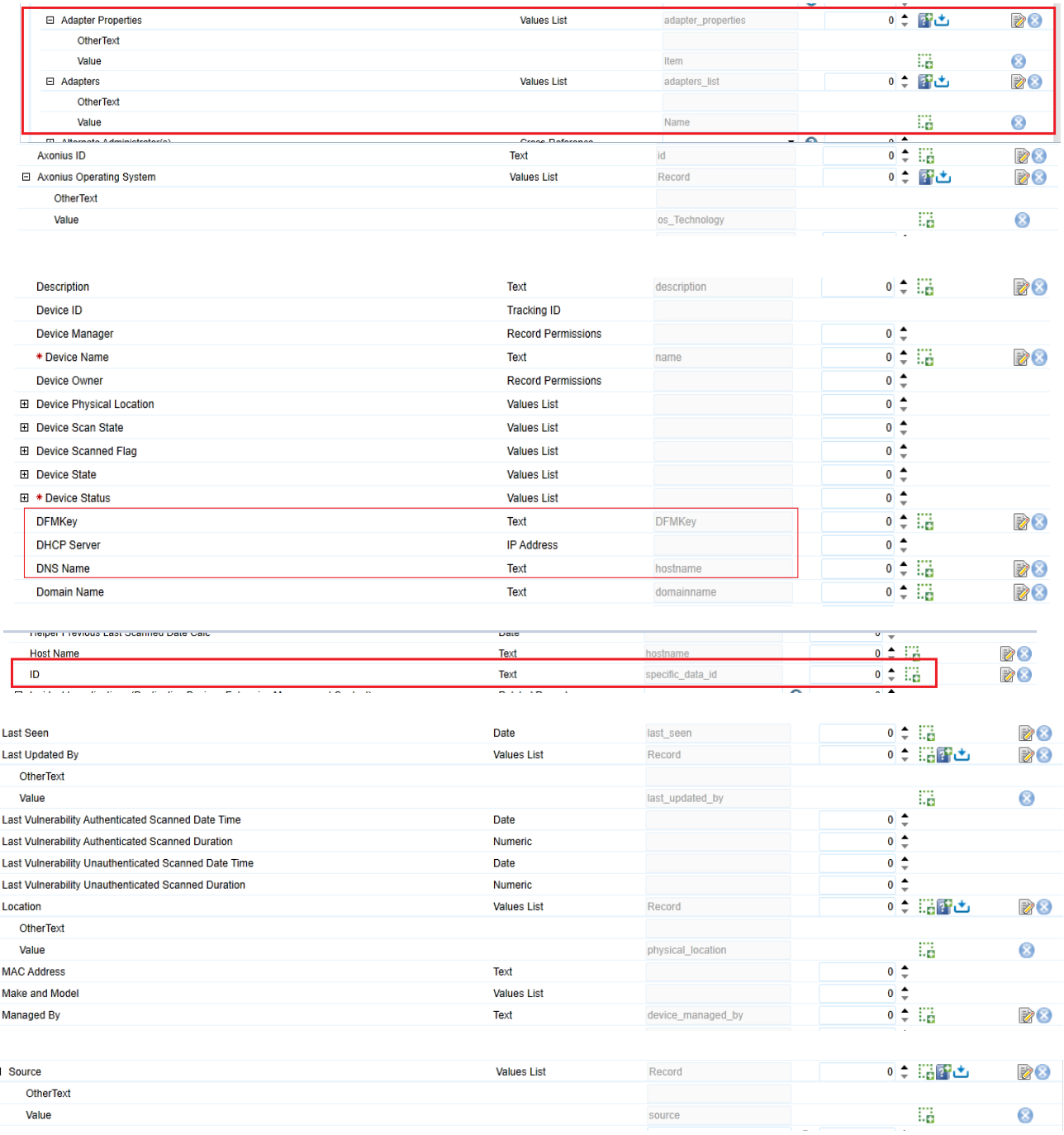
Key	Value
verifyCerts	[Valid value of true/false] Default = False

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
id	Axonius ID
specific_data_id	ID
last_seen	Last seen
adapter_properties	Adapter Properties
adapters_list	Adapters
device_managed_by	Managed By
os_technology	Axonius Operating System

The screen shots below provide examples of these field mappings.



13. In the Key Field Definitions Sub tab, add the “DFMKey” as key field for Devices.

Axonius integration helps create and update device records using a recommended method, to support the other ITSVP scanner integrations i.e. using a generic DFM key.
Here hostnames act as DNS names which forms the DFM key.
But when there is more than 1 hostname per device - the first one in the list is chosen for the data feed key field definition. Consequently, the devices with no hostnames would not be processed - But this can be modified based on your need. Hence this datafeed has been configured with XSLT transformation which could be exploited.

Upgrade Customers:

The latest data feed and JavaScript contains "DFM key" in the key field definition. This may create *duplicate* records if run as is because you had Axonius id as the key, but the uniqueness is based on DFM key now. Hence follow the below steps for the first run of the updated datafeed:

1. Import the latest data feed and the latest JavaScript.
2. For Data Mapping, please refer step 12 in the "Setup the Axonius Devices Data Feed" section above.
3. But for key field Definition retain the "Axonius id" as the Key and run the datafeed.
4. After successful completion of the datafeed, immediately change back the key field to "DFMKey" – for all future/subsequent runs.

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
Frequency	Specifies the interval in which the data feed runs. • **By minute:** Runs the data feed by the minute interval set. For example, if you specify 45 in every list, the data feed executes every 45 minutes. • **Hourly:** Runs the data feed by the hourly interval set. For example, every hour (1), every other hour (2), and so forth. • **Daily:** Runs the data feed by the daily internal set. For example, every day (1), every other day (2), and so forth. • **Weekly:** Runs the data feed based on a specified day of the week. For example, every Monday of the first week (1), every other Monday (2), and so forth. • **Monthly:** Runs the data feed based on a specified week of the month. For example, 1st, 2nd, 3rd, 4th, or Last. • **Reference:** Runs a specified data feed as runs before the current one. This option indicates to the Data Feed Service that this data feed starts as soon as the referenced data feed completes successfully. From the Reference Feed list, select after which existing data feed the current data feed starts. A reference data feed will not run when immediately running a data feed. The Data Feed Now option only runs the current data feed.
Every	Specifies the interval of the frequency in which the data feed runs.
Start Time	Specifies the time the data feed begins running.
Start Date	Specifies the date on which the data feed schedule begins.
Time Zone	Specifies the time zone in of the server that runs the data feed.

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
Archer Suite	Release 6.5 P2 and later up to 6.9 SP1	Virtual Appliance
Axonius	NA	NA