RSA® ARCHER® SUITE
Integration Guide

Tenable.sc Asset Discovery - RSA Archer Integration

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

License agreement

Third-party licenses

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

October 2019

Table of Contents

Chapter 1: Overview

About Tenable.sc

Tenable.sc provides your organization the ability to accurately identify, investigate, and prioritize vulnerabilities. With Tenable.sc you get a real-time, continuous assessment of your security posture so you can find, prioritize, and fix vulnerabilities faster.

The integration of Tenable.sc Asset Discovery with the Devices application in any of the below use cases enables customers to leverage the discovered devices and catalog those network devices within RSA Archer.

Key Features and Benefits

The Tenable.sc integration with RSA Archer enables organizations to:

- Catalog network devices on a corporate network.

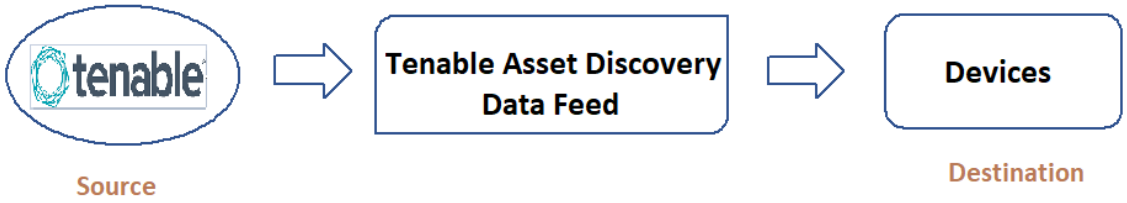
Requirements

Components	Requirement
RSA Archer Solution	• Audit Management • IT & Security Risk Management • Regulatory & Corporate Compliance Management • Third Party Management
RSA Archer Use Case(s)	The following use cases can take advantage of the information provided by the Tenable.sc integration: • RSA Archer Audit Engagements & Workpapers • RSA Archer Third Party Governance • RSA Archer Business Continuity & Disaster Recovery Planning • RSA Archer IT Controls Assurance • RSA Archer IT Security Vulnerability Program • RSA Archer IT Risk Management • RSA Archer Cyber Incident & Breach Response • RSA Archer PCI Management • RSA Archer Information Security Management System (ISMS) • RSA Archer Data Governance
RSA Archer Applications	Leverages the Devices application
Uses Custom Application	No
Requires On-Demand License	No
RSA Archer Requirements	Please refer “Tenable.sc Integration” page for version details

Components	Requirement
Tenable.sc Requirements	Valid Tenable.sc license is required

Integration Diagram

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



Chapter 2: Configure Tenable.sc Host

Configure the Data Feed

The following data feed is used as part of the Tenable.sc Integration process:

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

The data feeds must be configured. After setting up the data feed, you can schedule it to run **as needed per your organization's requirements**. For more information on scheduling the data feed, see the Scheduling Data Feed section.

Configure the JavaScript Transporter Settings

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

1. On the **General** tab, go to the **JavaScript Transporter** section.
   a. Open the **RSA 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 4b-4c for each thumbprint.
5. On the toolbar, click **Save**.

Obtaining Digital Thumbprints

When running JavaScript data feed, 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 Certificate 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**.

RSA Security LLC Certificate in the Trusted Root CA Store

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** subfolder of the **Trust Root Certification Authorities** folder.
3. In the **Certificates** subfolder, 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 window displays the following message:
   THIS certificate is OK.

   Note: If the Certificate Status window 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.

Download the Tenable.sc Vulnerabilities (Hosts) Data Feed

The Tenable.sc Hosts data feed can be downloaded from the Tenable.sc Integration exchange page: https://community.rsa.com/docs/DOC-95804

1. Open the above exchange page and click on the Integration Package.
2. Download the zip file.
3. Extract the zip file and copy the Security_Center_Vulns_(Hosts).dfx5 file.
4. Go to the "Tenable SecurityCenter Signed Javascripts" folder and copy the "SecurityCenterAPI.js" JavaScript file.
5. Paste both the files into your desired location, which will be used in this integration.

Note: Please refer to the Integration Package page for any package updates related to the Devices application. If you find that a new package is available, you must install it before configuring this data feed.

Setup the Tenable.sc Vulnerabilities (Hosts) Data Feed

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

Important: Updates to the API files used in the JavaScript Transporter (SecurityCenterAPI.js) can only be achieved in a hosted environment with a Professional Services engagement. For more information, contact your account representative.

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 **Security_Center_Vulns_(Hosts).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 **SecurityCenterAPI.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
Username	[Valid value]

Password	[Valid value]
dataSource	hosts
URL	[Valid value] For example, https://tenablesc.eastus.cloudapp.azure.com
ignoreLastRunTime	false
vulnSeverities	4,3,2,1
vulnDateFilterType	firstSeen
vulnLoadActive	true
vulnLoadPatched	true
verifyCerts	false

Note: The listed values are in place by default. They can be configured to suit your environment.
Important: The keys and values are case-sensitive and cannot include extra spaces at the end of the strings.

9. (Optional) Add startOffset as a new key.

   Note: The startOffset parameter specifies the first record in the range you want to retrieve, and the endOffset parameter specifies the last record in the range you want to retrieve. Use these parameters to parse data into consumable sizes. For more information, see the Tenable.sc API Best Practices Guide.

   a. Click **Add New**.
   b. Enter startOffset as the key.
   c. Define a valid value for the startOffset key.
   d. Click **Add New**.
   e. Enter endOffset at the key.
   f. Define a valid value for the endOffset key.

10. For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log.

11. Click the **Source Definition** tab.
    a. Click the **Tokens** subtab.
    b. Verify token values.

    The following table describes token values to verify.

Token	Value
BatchContentSave	1000
LastRunTime	(Populated by feed)
LastFileProcessed	(Populated by feed)
PreviousRunContext	(Populated by feed)

Note: For more information about tokens, see **Data Feed Tokens** in the **RSA Archer Online Documentation**.

12. Verify that key field values are not missing from the data feed setup window.
13. Click **Save**.

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 that 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 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. • **Reference:** Runs a specified data feed that will run 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 Tenable.sc were imported into the Devices application. If testing fails, try verifying the data feed and re-run the data feed. If you experience multiple failures, please contact your RSA Partner.

Appendix A: Certification Environment

Date Tested: September 2019

Product Name	Version Information	Operating System
RSA Archer Suite	Please refer "Tenable.sc Integration" page for version details	Virtual Appliance
Tenable.sc	NA	NA