Vendor Risk Management Module

SecurityScorecard Connector Administration Guide

Document Version: 03.01.01 | July 2019

Contents

About this Guide

The purpose of this Administration Guide is to describe implementation steps necessary to configure and operationalize SecurityScorecard Connector for Vendor Risk Management module.

This Administration Guide is intended to be used by technical stakeholders or Rsam administrators responsible for implementation of SecurityScorecard Connector.

SecurityScorecard Connector Requirements

The following software is required to use the SecurityScorecard Connector.

Supported Rsam Platform

Version 9.2 or higher.

Supported Vendor Risk Management Module

Version 3.0 or higher.

Setting up SecurityScorecard Connector

This section describes the high-level steps involved in setting up the SecurityScorecard Connector.

Prerequisites

The following are the requirements before setting up the SecurityScorecard Connector.

- The SecurityScorecard Connector configuration must be in your Rsam environment.
- The IP address of your Rsam web server must be whitelisted with SecurityScorecard. Contact your SecurityScorecard account manager for support.

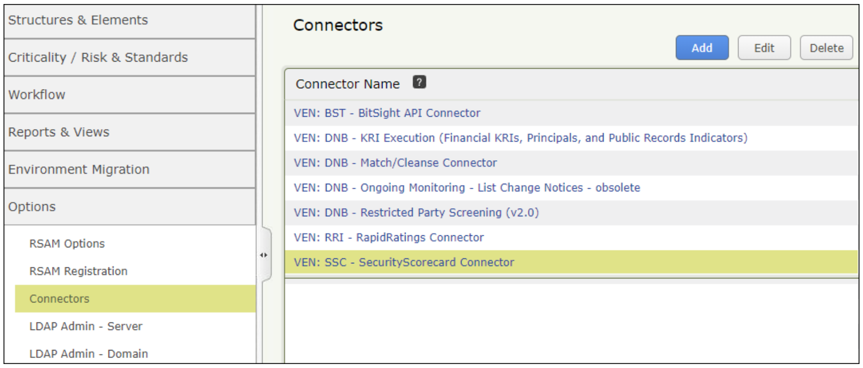
Update SecurityScorecard Connector Settings

To update the SecurityScorecard connector, perform the following steps:

1. Log in to your Rsam instance and go to **Manage** > **Administration**.

2. In the left navigation panel, click **Options** > **Connectors**.
   The list of connectors appears.

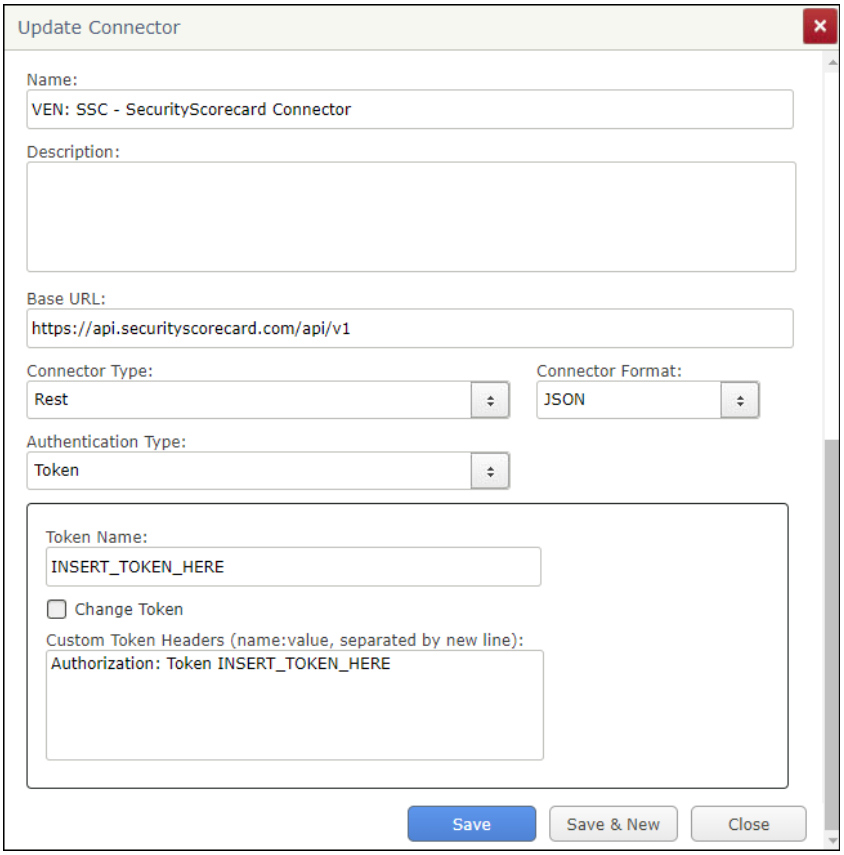
3. Select **VEN: SSC - SecurityScorecard Connector** and click **Edit**.



Connector Name
VEN: BST - BitSight API Connector
VEN: DNB - KRI Execution (Financial KRIs, Principals, and Public Records Indicators)
VEN: DNB - Match/Cleanse Connector
VEN: DNB - Ongoing Monitoring - List Change Notices - obsolete
VEN: DNB - Restricted Party Screening (v2.0)
VEN: RRI - RapidRatings Connector
VEN: SSC - SecurityScorecard Connector

The **Update Connector** dialog box appears.

4. Enter the name of the token in the **Token Name** field.



Name: VEN: SSC - SecurityScorecard Connector

Description:

Base URL: https://api.securityscorecard.com/api/v1

Connector Type: Rest

Connector Format: JSON

Authentication Type: Token

Token Name: INSERT_TOKEN_HERE

□ Change Token

Custom Token Headers (name:value, separated by new line):

Authorization: Token INSERT_TOKEN_HERE

5. If you want to change the token, select the **Change Token** check box and enter the token in **Token** and **Confirm Token** fields.

6. Enter the connection token information in the **Custom Token Headers** field. If you do not have the token information, contact your SecurityScorecard Account Manager.

7. Click **Save**. The connector is updated with the configuration.

Thresholds to Create Alerts

Event handlers are created for the following two purposes:

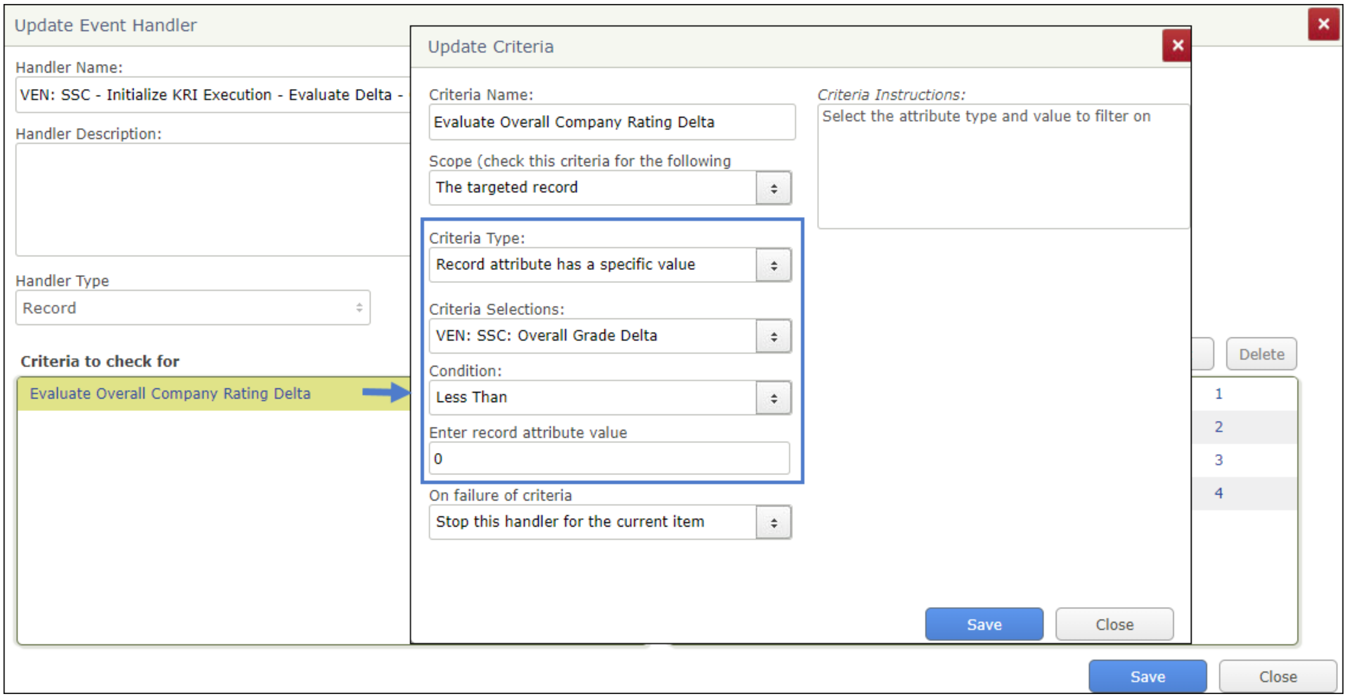
- To generate alerts when the current rating goes below the previously recorded rating of a vendor
- To track vendor health over time

In this section, you will get familiar with the event handlers and learn about the out-of-the-box configuration.

Overall Company Grade Value

The **VEN: SSC - Initialize KRI Execution - Evaluate Delta - Overall Company Rating** event handler will generate an alert if the overall company rating (**VEN: SSC: Overall Grade Delta**) of the vendor goes below the threshold value entered for the record attribute value in the event handler criteria. The out-of-the-box configuration of the handler is to generate an alert when the current Overall Grade value goes below the last generated Overall Grade (i.e. **VEN: SSC: Overall Grade Delta** is less than 0).

The following screenshot shows the handler and the criteria.



Update Event Handler

Handler Name: VEN: SSC - Initialize KRI Execution - Evaluate Delta -

Handler Description:

Handler Type: Record

Criteria to check for

Evaluate Overall Company Rating Delta

Update Criteria

Criteria Name: Evaluate Overall Company Rating Delta

Criteria Instructions: Select the attribute type and value to filter on

Scope (check this criteria for the following: The targeted record

Criteria Type: Record attribute has a specific value

Criteria Selections: VEN: SSC: Overall Grade Delta

Condition: Less Than

Enter record attribute value: 0

On failure of criteria: Stop this handler for the current item

Modifying a Threshold

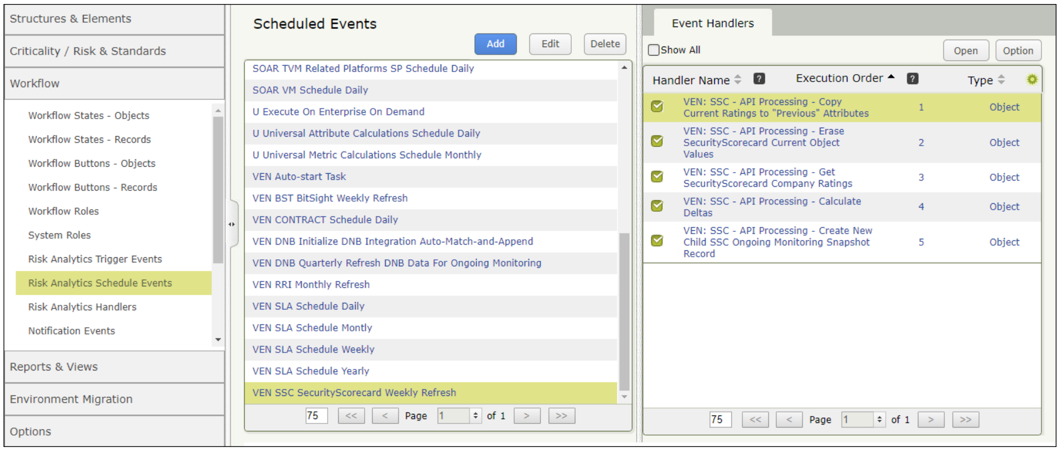
To modify a threshold, perform the following steps:

1. In the left navigation panel, click **Workflow** > **Risk Analytics Handlers**.
2. Search for the event handler you wish to edit.
3. Select the event handler and click **Edit**.
4. Select the criteria and click **Edit**.
5. Modify the criteria as required and click **Save**.
6. Click **Save** to exit the **Update Event Handler** dialog box.

Setting up the Scheduler

In this step, you will create a new schedule to execute the **VEN SSC SecurityScorecard Weekly Refresh** scheduled event (task) and pull the latest SecurityScorecard ratings automatically for a set of vendors without any intervention for unattended use. To create a new schedule, perform the following steps:

1. In the left navigation panel, click **Workflow** > **Risk Analytics Schedule Events**.



Structures & Elements
Criticality / Risk & Standards
Workflow
- Workflow States - Objects
- Workflow States - Records
- Workflow Buttons - Objects
- Workflow Buttons - Records
- Workflow Roles
- System Roles
- Risk Analytics Trigger Events
- Risk Analytics Schedule Events
- Risk Analytics Handlers
- Notification Events

Reports & Views
Environment Migration
Options

Scheduled Events

Add | Edit | Delete

- SOAR TVM Related Platforms SP Schedule Daily
- SOAR VM Schedule Daily
- U Execute On Enterprise On Demand
- U Universal Attribute Calculations Schedule Daily
- U Universal Metric Calculations Schedule Monthly
- VEN Auto-start Task
- VEN BST BitSight Weekly Refresh
- VEN CONTRACT Schedule Daily
- VEN DNB Initialize DNB Integration Auto-Match-and-Append
- VEN DNB Quarterly Refresh DNB Data For Ongoing Monitoring
- VEN RRI Monthly Refresh
- VEN SLA Schedule Daily
- VEN SLA Schedule Montly
- VEN SLA Schedule Weekly
- VEN SLA Schedule Yearly
- VEN SSC SecurityScorecard Weekly Refresh

75 | << | < | Page 1 of 1 | > | >>

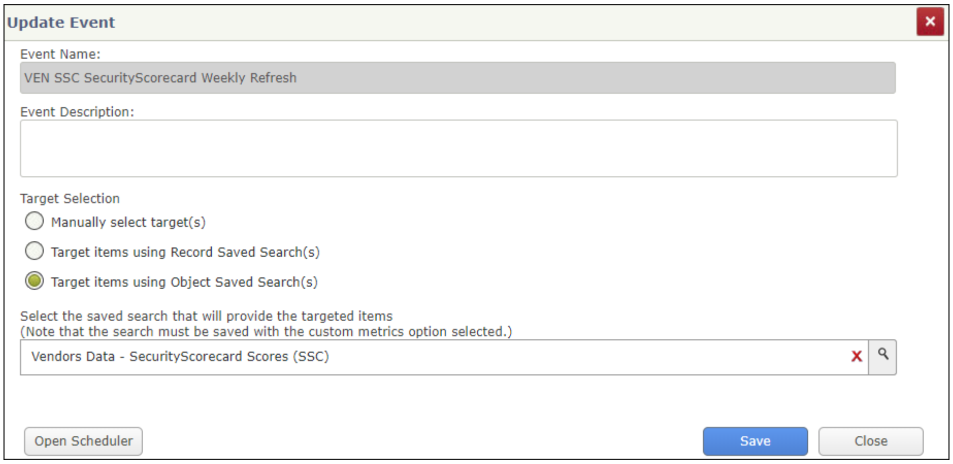
Event Handlers

□ Show All | Open | Option

	Handler Name	Execution Order	Type
☑	VEN: SSC - API Processing - Copy Current Ratings to "Previous" Attributes	1	Object
☑	VEN: SSC - API Processing - Erase SecurityScorecard Current Object Values	2	Object
☑	VEN: SSC - API Processing - Get SecurityScorecard Company Ratings	3	Object
☑	VEN: SSC - API Processing - Calculate Deltas	4	Object
☑	VEN: SSC - API Processing - Create New Child SSC Ongoing Monitoring Snapshot Record	5	Object

75 | << | < | Page 1 of 1 | > | >>

2. Double-click the **VEN SSC SecurityScorecard Weekly Refresh** scheduled event to open the **Update Event** dialog box.



Update Event

Event Name: VEN SSC SecurityScorecard Weekly Refresh

Event Description:

Target Selection
- ○ Manually select target(s)
- ○ Target items using Record Saved Search(s)
- ● Target items using Object Saved Search(s)

Select the saved search that will provide the targeted items
(Note that the search must be saved with the custom metrics option selected.)

Vendors Data - SecurityScorecard Scores (SSC)

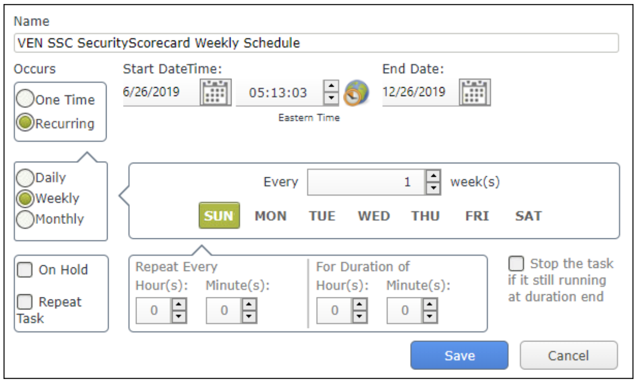
Open Scheduler | Save | Close

3. Click **Open Scheduler**. The **Scheduler** dialog box appears.

4. Go to **Schedules** and click **Add**. The **Add/Modify Schedule** dialog box appears.

5. Provide values for the fields as listed in the following table.

Field Name	Value(s)
Name	VEN SSC SecurityScorecard Weekly Schedule
Start Date Time	Select the date to begin running the schedule.
End Date	Select the date to stop running the schedule (this can be several years in the future).
Occurs	Select **Recurring – Weekly – SUN**



Name: VEN SSC SecurityScorecard Weekly Schedule

Occurs: ○ One Time ● Recurring

Start DateTime: 6/26/2019 05:13:03 Eastern Time

End Date: 12/26/2019

○ Daily ● Weekly ○ Monthly

Every 1 week(s)

SUN MON TUE WED THU FRI SAT

□ On Hold

□ Repeat Task

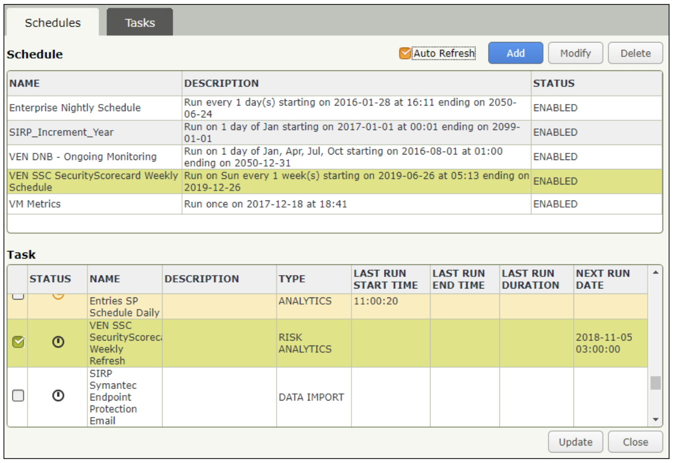
Repeat Every Hour(s): 0 Minute(s): 0

For Duration of Hour(s): 0 Minute(s): 0

□ Stop the task if it still running at duration end

6. Click **Save**. The scheduler configuration is saved.

7. Associate the schedule (**VEN SSC SecurityScorecard Weekly Schedule**) to the task (**VEN SSC SecurityScorecard Weekly Refresh**).



Schedule

NAME	DESCRIPTION	STATUS
Enterprise Nightly Schedule	Run every 1 day(s) starting on 2016-01-28 at 16:11 ending on 2050-06-24	ENABLED
SIRP_Increment_Year	Run on 1 day of Jan starting on 2017-01-01 at 00:01 ending on 2099-01-01	ENABLED
VEN DNB - Ongoing Monitoring	Run on 1 day of Jan, Apr, Jul, Oct starting on 2016-08-01 at 01:00 ending on 2050-12-31	ENABLED
VEN SSC SecurityScorecard Weekly Schedule	Run on Sun every 1 week(s) starting on 2019-06-26 at 05:13 ending on 2019-12-26	ENABLED
VM Metrics	Run once on 2017-12-18 at 18:41	ENABLED

Task

	STATUS	NAME	DESCRIPTION	TYPE	LAST RUN START TIME	LAST RUN END TIME	LAST RUN DURATION	NEXT RUN DATE
□		Entries SP Schedule Daily		ANALYTICS	11:00:20			
☑		VEN SSC SecurityScorec; Weekly Refresh		RISK ANALYTICS				2018-11-05 03:00:00
□		SIRP Symantec Endpoint Protection Email		DATA IMPORT				

8. Click **Update** and close the dialog box. The schedule is saved.

Working with the SecurityScorecard Connector

This section will walk you through the use cases, dashboards, and the procedure to respond alerts.

SecurityScorecard Connector Use Cases

The SecurityScorecard Connector supports both attended and unattended use cases.

SecurityScorecard Data within Vendor/Service Profile – Attended Use

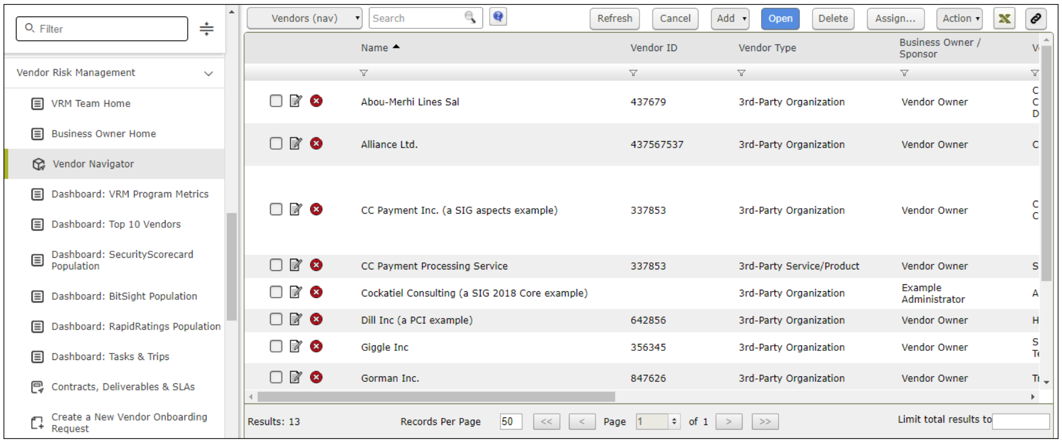
In the attended use case, you will actively engage with a vendor/service object to get SecurityScorecard data. This interaction is possible from within an individual vendor/service profile view or by selecting multiple vendors/services in a list.

To get latest SecurityScorecard data within a vendor/service, perform the following steps:

1. In the left navigation panel, click **Vendor Risk Management** > **Vendor Navigator**.

   The vendor list appears.

2. Select a vendor and click **Open**.

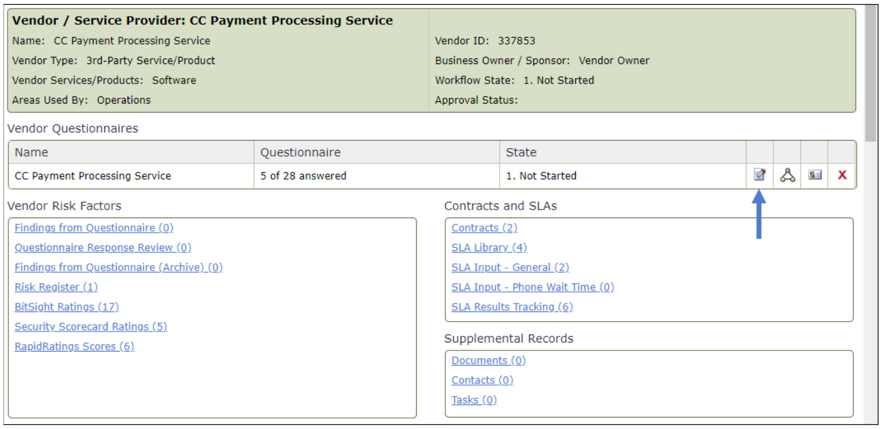

Filter
Vendor Risk Management
VRM Team Home
Business Owner Home
Vendor Navigator
Dashboard: VRM Program Metrics
Dashboard: Top 10 Vendors
Dashboard: SecurityScorecard Population
Dashboard: BitSight Population
Dashboard: RapidRatings Population
Dashboard: Tasks & Trips
Contracts, Deliverables & SLAs
Create a New Vendor Onboarding Request
Vendors (nav)
Search
Refresh
Cancel
Add
Open
Delete
Assign...
Action

	Name ▲	Vendor ID	Vendor Type	Business Owner / Sponsor	V
□	Abou-Merhi Lines Sal	437679	3rd-Party Organization	Vendor Owner	C C D
□	Alliance Ltd.	437567537	3rd-Party Organization	Vendor Owner	C
□	CC Payment Inc. (a SIG aspects example)	337853	3rd-Party Organization	Vendor Owner	C C
□	CC Payment Processing Service	337853	3rd-Party Service/Product	Vendor Owner	S
□	Cockatiel Consulting (a SIG 2018 Core example)		3rd-Party Organization	Example Administrator	A
□	Dill Inc (a PCI example)	642856	3rd-Party Organization	Vendor Owner	H
□	Giggle Inc	356345	3rd-Party Organization	Vendor Owner	S Te
□	Gorman Inc.	847626	3rd-Party Organization	Vendor Owner	Ti

Results: 13 Records Per Page 50 << < Page 1 of 1 > >> Limit total results to

The vendor details page appears.

3. In the **Vendor Questionnaires** section, choose a questionnaire and click **Open Questionnaire** icon.



Vendor / Service Provider: CC Payment Processing Service

Name: CC Payment Processing Service
Vendor Type: 3rd-Party Service/Product
Vendor Services/Products: Software
Areas Used By: Operations
Vendor ID: 337853
Business Owner / Sponsor: Vendor Owner
Workflow State: 1. Not Started
Approval Status:

Vendor Questionnaires

Name	Questionnaire	State
CC Payment Processing Service	5 of 28 answered	1. Not Started

Vendor Risk Factors

- Findings from Questionnaire (0)
- Questionnaire Response Review (0)
- Findings from Questionnaire (Archive) (0)
- Risk Register (1)
- BitSight Ratings (17)
- Security Scorecard Ratings (5)
- RapidRatings Scores (6)

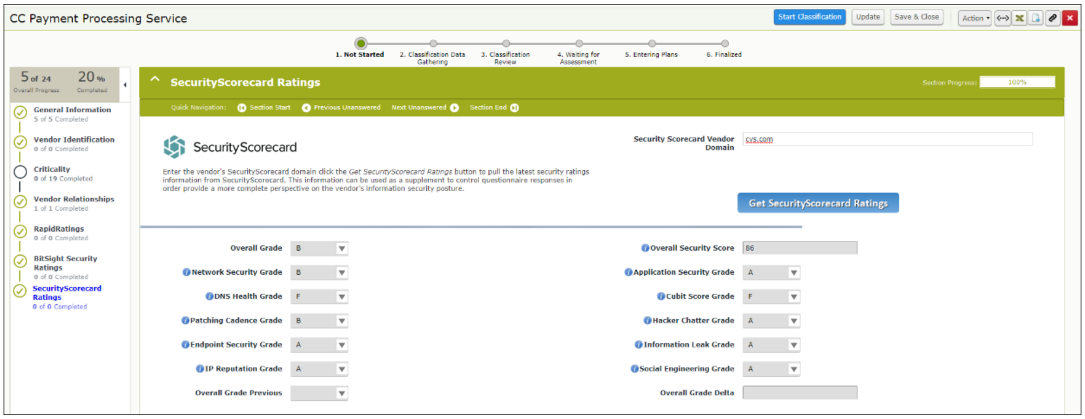
Contracts and SLAs

- Contracts (2)
- SLA Library (4)
- SLA Input - General (2)
- SLA Input - Phone Wait Time (0)
- SLA Results Tracking (6)

Supplemental Records

- Documents (0)
- Contacts (0)
- Tasks (0)

4. In the left panel, click **SecurityScorecard Ratings** and then click **Get SecurityScorecard Ratings** on the main page.



CC Payment Processing Service
Start Classification
Update
Save & Close
Action
1. Not Started
2. Classification Data Gathering
3. Classification Review
4. Waiting for Assessment
5. Entering Plans
6. Finalized
5 of 24 Overall Progress
20 % Completed
General Information 5 of 5 Completed
Vendor Identification 0 of 0 Completed
Criticality 0 of 19 Completed
Vendor Relationships 1 of 1 Completed
RapidRatings 0 of 0 Completed
BitSight Security Ratings 0 of 0 Completed
SecurityScorecard Ratings 0 of 0 Completed
SecurityScorecard Ratings
Section Progress: 100%
Quick Navigation: Section Start Previous Unanswered Next Unanswered Section End
SecurityScorecard
Get SecurityScorecard Ratings

Enter the vendor's SecurityScorecard domain click the *Get SecurityScorecard Ratings* button to pull the latest security ratings information from SecurityScorecard. This information can be used as a supplement to control questionnaire responses in order provide a more complete perspective on the vendor's information security posture.

Security Scorecard Vendor Domain: cvs.com

Overall Grade	B	Overall Security Score	86
Network Security Grade	B	Application Security Grade	A
DNS Health Grade	F	Cubit Score Grade	F
Patching Cadence Grade	B	Hacker Chatter Grade	A
Endpoint Security Grade	A	Information Leak Grade	A
IP Reputation Grade	A	Social Engineering Grade	A
Overall Grade Previous		Overall Grade Delta	

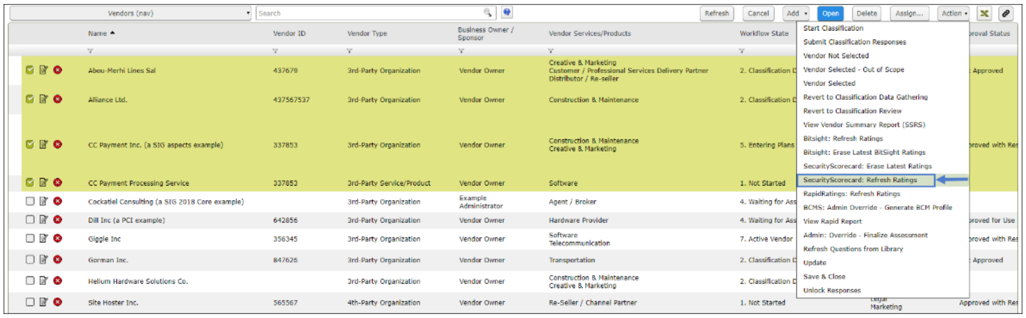
Rsam will now pull the latest ratings from SecurityScorecard.

To get the latest SecurityScorecard data for multiple vendors / services, perform the following steps:

1. In the left navigation panel, click **Vendor Risk Management** > **Vendor Navigator**.
   The vendor list appears.

2. Select the check box for each vendor/service you wish to get the latest SecurityScorecard data.

3. Click **Action** and select **SecurityScorecard: Refresh Ratings**.


Vendors (nav)
Search
Refresh
Cancel
Add
Open
Delete
Assign...
Action
Start Classification
Submit Classification Responses
Vendor Not Selected
Vendor Selected - Out of Scope
Vendor Selected
Revert to Classification Data Gathering
Revert to Classification Review
View Vendor Summary Report (SSRS)
Bitsight: Refresh Ratings
Bitsight: Erase Latest BitSight Ratings
SecurityScorecard: Erase Latest Ratings
SecurityScorecard: Refresh Ratings
RapidRatings: Refresh Ratings
BCMS: Admin Override - Generate BCM Profile
View Rapid Report
Admin: Override - Finalize Assessment
Refresh Questions from Library
Update
Save & Close
Unlock Responses

	Name ▲	Vendor ID	Vendor Type	Business Owner / Sponsor	Vendor Services/Products	Workflow State		roval Status
☑	Abou-Merhi Lines Sal	437679	3rd-Party Organization	Vendor Owner	Creative & Marketing Customer / Professional Services Delivery Partner Distributor / Re-seller	2. Classification D		: Approved
☑	Alliance Ltd.	437567537	3rd-Party Organization	Vendor Owner	Construction & Maintenance	2. Classification D		
☑	CC Payment Inc. (a SIG aspects example)	337853	3rd-Party Organization	Vendor Owner	Construction & Maintenance Creative & Marketing	5. Entering Plans		proved with Res
☑	CC Payment Processing Service	337853	3rd-Party Service/Product	Vendor Owner	Software	1. Not Started		
☐	Cockatiel Consulting (a SIG 2018 Core example)		3rd-Party Organization	Example Administrator	Agent / Broker	4. Waiting for Ass		
☐	Dill Inc (a PCI example)	642856	3rd-Party Organization	Vendor Owner	Hardware Provider	4. Waiting for Ass		proved for Use
☐	Giggle Inc	356345	3rd-Party Organization	Vendor Owner	Software Telecommunication	7. Active Vendor		proved with Res
☐	Gorman Inc.	847626	3rd-Party Organization	Vendor Owner	Transportation	2. Classification D		: Approved
☐	Helium Hardware Solutions Co.		3rd-Party Organization	Vendor Owner	Construction & Maintenance Creative & Marketing	2. Classification D		
☐	Site Hoster Inc.	565567	4th-Party Organization	Vendor Owner	Re-Seller / Channel Partner	1. Not Started	Legal Marketing	Approved with Res

The ratings are refreshed.

SecurityScorecard Data within Vendor/Service Profile – Unattended Use

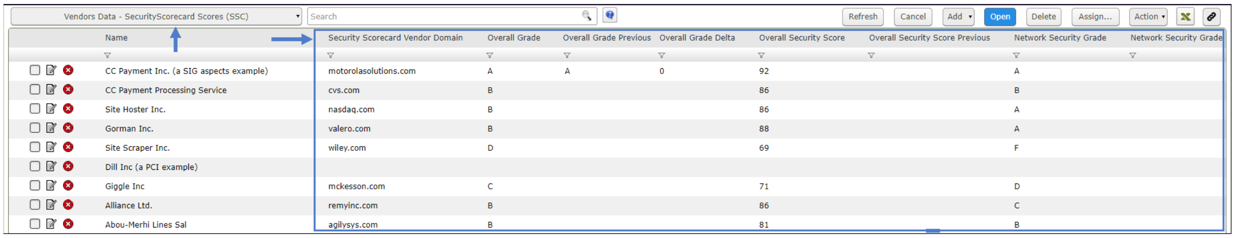
In the unattended use case, the SecurityScorecard Connector is scheduled to run for a pre-defined set of vendors. Without user intervention, the scheduler (that was set up in the earlier section of this document) pulls SecurityScorecard scores for all vendors and results are available on the **Vendors Data – SecurityScorecard Security Scores (SSC)** object search to help you monitor the ratings.

To access the SecurityScorecard Vendor ratings, perform the following steps:

1. In the left navigation panel, click **Vendor Risk Management** > **Vendor Navigator**.

   The vendor list appears.

2. In the navigation type, select **Vendors Data – SecurityScorecard Scores (SSC)**.



	Name	Security Scorecard Vendor Domain	Overall Grade	Overall Grade Previous	Overall Grade Delta	Overall Security Score	Overall Security Score Previous	Network Security Grade	Network Security Grade
☐	CC Payment Inc. (a SIG aspects example)	motorolasolutions.com	A	A	0	92		A	
☐	CC Payment Processing Service	cvs.com	B			86		B	
☐	Site Hoster Inc.	nasdaq.com	B			86		A	
☐	Gorman Inc.	valero.com	B			88		A	
☐	Site Scraper Inc.	wiley.com	D			69		F	
☐	Dill Inc (a PCI example)								
☐	Giggle Inc	mckesson.com	C			71		D	
☐	Alliance Ltd.	remyinc.com	B			86		C	
☐	Abou-Merhi Lines Sal	agilysys.com	B			81		B	

The vendor list with the rating information appears.

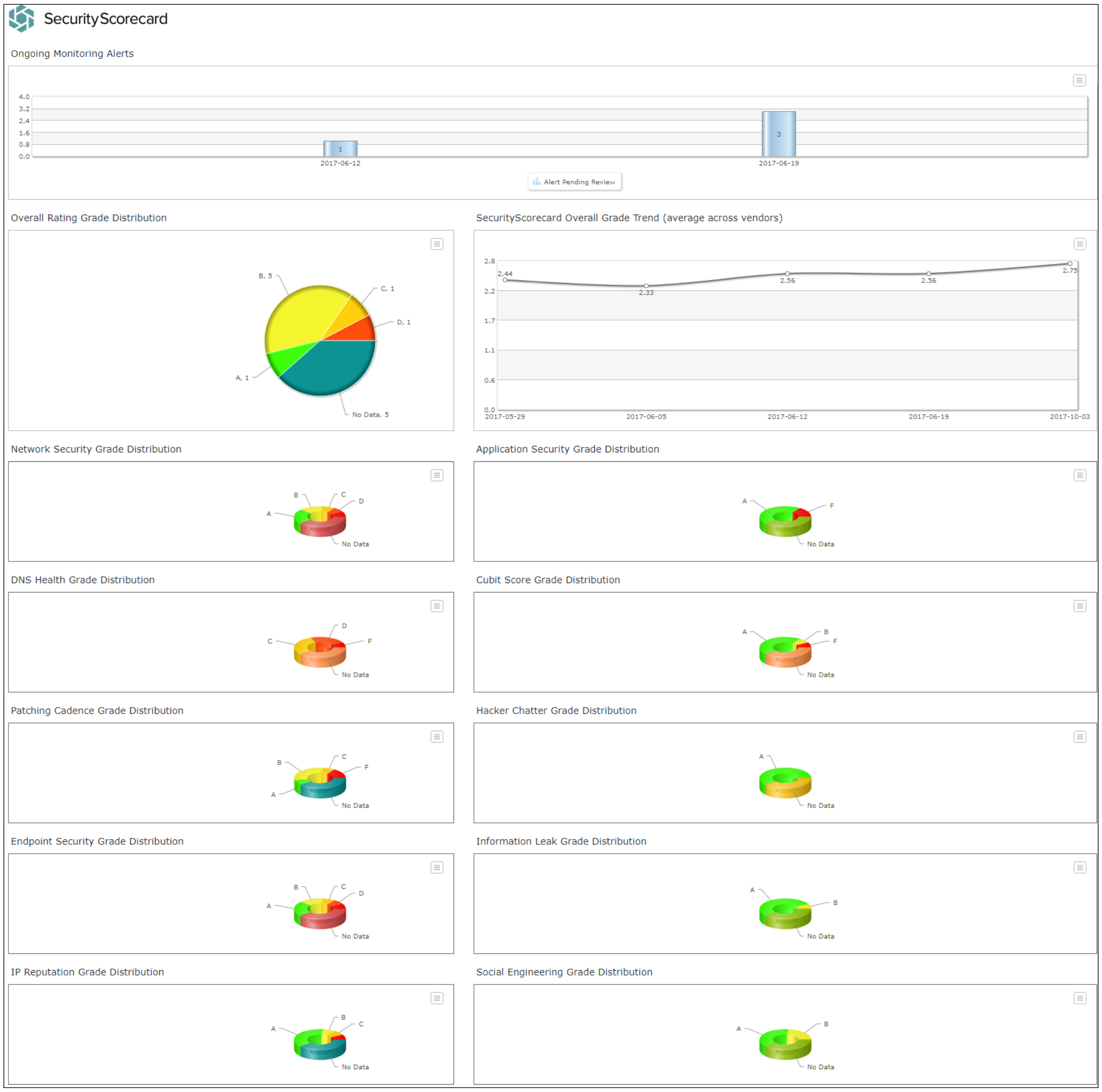
SecurityScorecard Dashboards and Views

This section provides an overview of the dashboards and views available for the SecurityScorecard Connector.

Dashboard: SecurityScorecard Population

This dashboard contains charts that illustrate SecurityScorecard overall rating grade distribution and the overall grade trend across all vendors. The charts also provide information such as grade distribution of network security, application security, DNS Health, and Cubit Score.

To access this dashboard, in the left navigation panel, click **Vendor Risk Management** > **Dashboard: SecurityScorecard Population**.


SecurityScorecard
Ongoing Monitoring Alerts
4.0
3.2
2.4
1.6
0.8
0.0
1
3
2017-06-12
2017-06-19
Alert Pending Review
Overall Rating Grade Distribution
B, 5
C, 1
D, 1
A, 1
No Data, 5
SecurityScorecard Overall Grade Trend (average across vendors)
2.8
2.2
1.7
1.1
0.6
0.0
2.44
2.33
2.56
2.56
2.75
2017-05-29
2017-06-05
2017-06-12
2017-06-19
2017-10-03
Network Security Grade Distribution
B
C
D
A
No Data
Application Security Grade Distribution
A
F
No Data
DNS Health Grade Distribution
D
C
F
No Data
Cubit Score Grade Distribution
A
B
F
No Data
Patching Cadence Grade Distribution
C
B
F
A
No Data
Hacker Chatter Grade Distribution
A
No Data
Endpoint Security Grade Distribution
B
C
D
A
No Data
Information Leak Grade Distribution
A
B
No Data
IP Reputation Grade Distribution
B
C
A
No Data
Social Engineering Grade Distribution
A
B
No Data

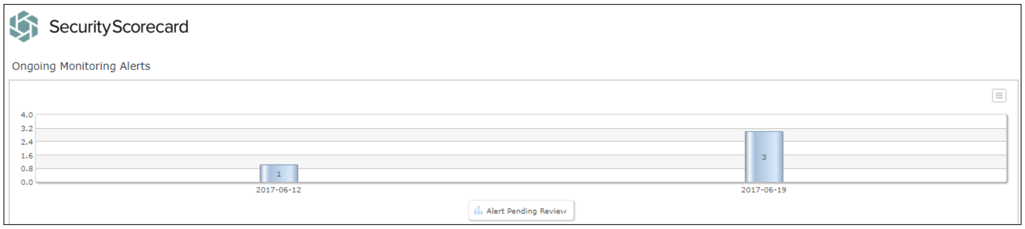
Monitoring Alerts

When the ratings go below the threshold values, alerts are created as records.

To review the alerts, perform the following steps:

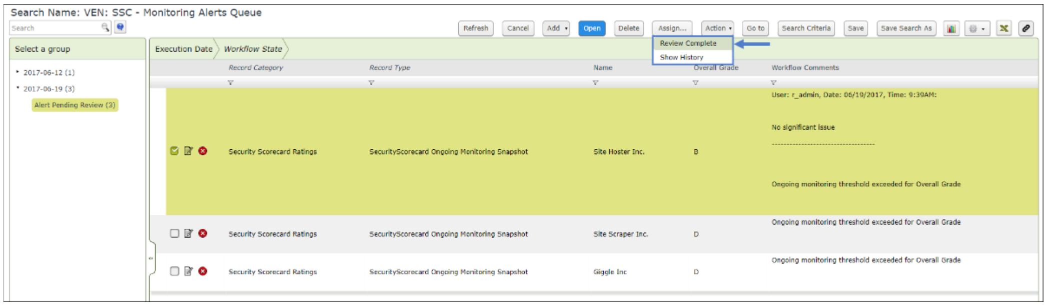
1. In the left navigation panel, click **Vendor Risk Management** > **Dashboard: SecurityScorecard Population**.

2. Click the data bar (in light blue) illustrating **Alerts Pending Review**.



The **VEN: SSC - Monitoring Alerts Queue** appears.

3. Select a record and click **Action** > **Review Complete**.



Search Name: VEN: SSC - Monitoring Alerts Queue

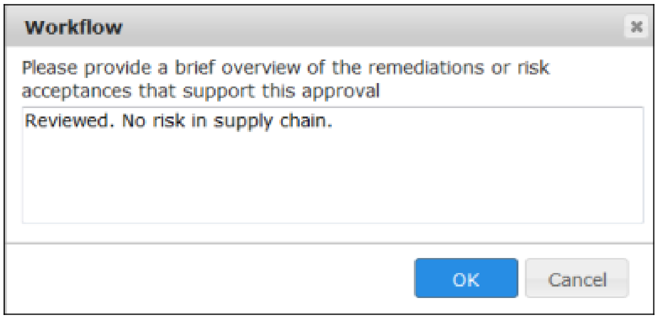
Select a group
- 2017-06-12 (1)
- 2017-06-19 (3)
  - Alert Pending Review (3)

Execution Date > Workflow State

	Record Category	Record Type	Name	Overall Grade	Workflow Comments
☑	Security Scorecard Ratings	SecurityScorecard Ongoing Monitoring Snapshot	Site Hoster Inc.	B	User: r_admin, Date: 06/19/2017, Time: 9:39AM: No significant issue ---------------------------------- Ongoing monitoring threshold exceeded for Overall Grade
□	Security Scorecard Ratings	SecurityScorecard Ongoing Monitoring Snapshot	Site Scraper Inc.	D	Ongoing monitoring threshold exceeded for Overall Grade
□	Security Scorecard Ratings	SecurityScorecard Ongoing Monitoring Snapshot	Giggle Inc	D	Ongoing monitoring threshold exceeded for Overall Grade

The **Workflow** dialog box appears.

4. Enter an overview of the review and click **OK**.



Workflow

Please provide a brief overview of the remediations or risk acceptances that support this approval

Reviewed. No risk in supply chain.

Appendix: Rsam Documentation

Vendor Risk Management Tutorial

For a detailed walk-through of the Vendor Risk Management user experience, refer to the *Vendor Risk Management Step-by-Step Tutorial*. You should have received the *Vendor Risk Management Step-by-Step Tutorial* along with the Vendor Risk Management instance. If not, contact your Rsam Customer Representative to obtain an electronic copy of the *Vendor Risk Management Step-by-Step Tutorial*.

Online Help

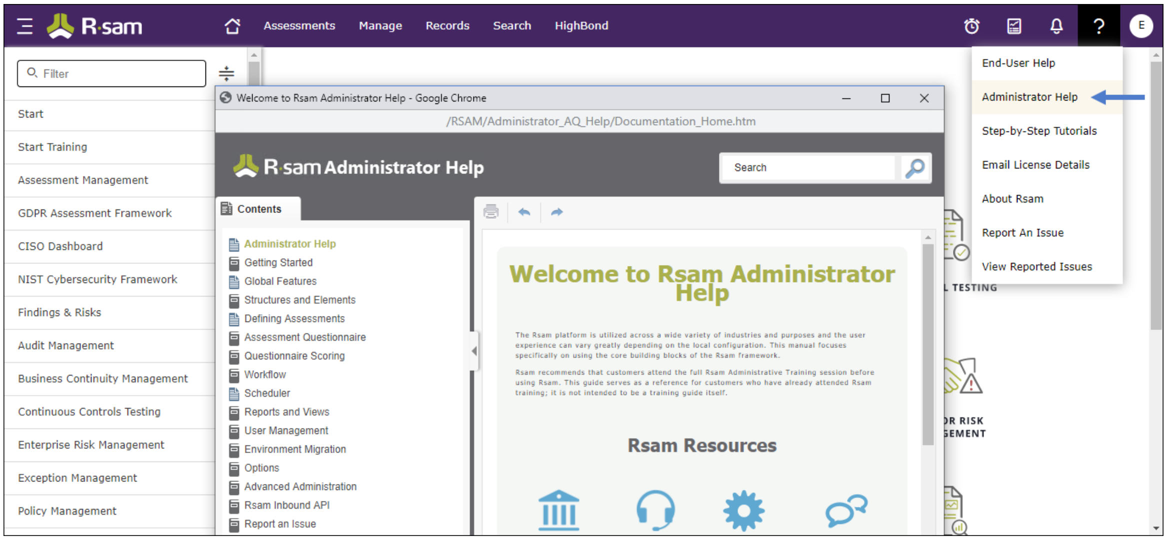
To get familiar with the specific Rsam features used in this configuration, refer to the *Rsam End-User Help*, *Rsam Administrator Help*, or both. The Online help you can access depends on your user permissions.

To access the Online Help, perform the following steps:

1. Sign in to your Rsam instance. For example, sign in as *Example Administrator* user. Provide the **Username** as **r_admin** and **Password** as **password**.

2. Hover the cursor over **Help** and select an Online help from the menu that appears. Depending on your user permissions, you will be able to access the Rsam End-User Help, Rsam Administrator Help, Step-by-Step Tutorials, or all.

   The following image shows the *Rsam Administrator Help*, opened from the *Example Administrator* user account.



Welcome to Rsam Administrator Help

The Rsam platform is utilized across a wide variety of industries and purposes and the user experience can vary greatly depending on the local configuration. This manual focuses specifically on using the core building blocks of the Rsam framework.

Rsam recommends that customers attend the full Rsam Administrative Training session before using Rsam. This guide serves as a reference for customers who have already attended Rsam training; it is not intended to be a training guide itself.

Rsam Resources