RSA Archer GRC

Release Notes

Security Incident Management 1.0 and Later

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 towww.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.

November 2017

Table of Contents

Preface

This is a cumulative document that contains all of the Release Notes for the RSA® Archer® Security Incident Management release 1 and subsequent releases, service packs and patches. The document is organized in chronological order from the latest release to the earliest release.

These Release Notes may be updated. The most current version can be found on the RSA Archer Community on RSA Link.

The audience for this document is the RSA Archer GRC administrator.

Upgrading from Release 1.0

When you upgrade from Security Incident Management 1.0 to any later version, you must perform the following steps:

1. Export Incident Response Procedures from SOC Procedure Library
2. Separate Incident Response Procedures and Tasks
3. Import Migrated Data into Incident Response Procedures Library Application
4. Import Migrated Data into Incident Response Procedures Application

Export Incident Response Procedures from SOC Procedure Library

In the release1.1 and later, the SOC Procedure Library was renamed to Incident Response Procedure Library and was changed to a leveled application. You must export and delete your Incident Response Procedures prior to upgrading. Separate and import them into the Incident Response Procedure Library application and Incident Response Procedure application post upgrade.

Procedure

1. From the Navigation Menu, expand the SOC Procedure Library application and click Search Records.
2. In the Fields to Display section, from the Available menu, select the following required fields:
   - Name
   - Description
   - Incident Categories
   - Priority
   - Required/Optional
   - Target
3. In the Filters section, enter the following values, in order, to search for only the incident response procedures.

Filter	Value
Field to Evaluate Type	Type
Operator Equals	Equals
Values Incident	Incident

4. Click Search
5. Click Export.
6. In the Export Options dialog, select CSV.
7. In the Warning pop-up, select Exclude HTML formatting tags.
8. Click OK.
9. Save your file as Incident_Response_Procedures.CSV.
   Important: Note the name and location of your file. You will need it for later tasks.
10. Delete the incident response procedures from the SOC Procedure Library.

Export Incident Response Tasks from the Incident Response Task Application

In version 1.1, the Incident Response Tasks application was changed to a leveled application. By default when a flat application changes to a leveled application, any previously existing data is stored at the parent level and data that belongs in the child level must be manually imported into the correct level. If you are upgrading from RSA Archer Security Incident Management 1.0, you must complete this task to ensure that your data is migrated correctly.

Procedure

1. From the Navigation Menu, select Incident Response > Incident Response Tasks.
2. Click Advanced Search to search records.
3. In the Fields to Display section, from the Available menu, select the following required fields:
    - Name
    - Analyst name
    - Analyst Notes
    - Description
    - Implementation Status
    - Order
    - Related Investigation
    - Related Security Incident
    - Required/Optional
    - Target Analyst
    - Threat Category
4. Click Search
5. Click Export.
6. In the Export Options dialog, select CSV.
7. In the Warning pop-up, select Exclude all HTML formatting tags.
8. Click OK.
9. Save the CSV file as Incident_Response_Task.
   Important: Note the name and location of your file. You will need it for later tasks.

Separate Incident Response Procedures and Tasks

After exporting your existing incident response procedure data, you must separate the incident response procedures from the incident response tasks. RSA strongly recommends contacting Professional Services for assistance.

Procedure

1. Open the Incident_Response_Procedures.CSV file.
2. Copy and paste the following procedure information into a separate new CSV file. Save the CSV file as Separated_Procedures.CSV.
    - Procedure Name (Mandatory)
    - Description (Mandatory)
    - Incident Categories/Threat Categories (Mandatory)
    - Procedure Status (Mandatory for Incident Response Procedure library application)
      Note: This field must be populated manually. Populate the field as Active for all active records and Inactive for all inactive records.
    - Link to Security Incidents (Optional)
3. Open the Incident_Response_Task.CSVfile.
4. Copy and paste the following task information into a separate new CSV file. Save the CSV file as Separated_Task.CSV.
    - Task Name (Mandatory)
    - Description (Mandatory)
    - Step Number – Order field from 1.0 (Mandatory)
    - Required/Optional (Mandatory)
    - Target – Must be populated from Groups (Mandatory)
    - Analyst Name (Optional)
    - Analyst Notes (Optional)
    - Link to Security Incidents (Optional)

Import Migrated Data into the Incident Response Procedure Library

Procedure

1. Locate the CSV files you created and saved in ***Separate Incident Response Procedures and Tasks***, Separated_Procedures.CSV and Separated_Task.CSV.
2. From the Navigation Menu, select Administration > Integration > Manage Data Imports.
3. In the Incident Response Procedure Library, do one of the following:
    a. If you are importing your incident response procedures, select the Incident Response Procedure level.
    b. If you are importing your incident response tasks, select the incident Response Task level.
4. In the Data Import Wizard, in the General Information section, select Browse.
5. From the File Upload window, click Add New.
6. Select the Separated_Procedures.CSV file that you created and saved earlier (Separate Incident Response Procedures and Tasks).
7. In the Formal Options section, leave all the fields as default, and click Next.
8. From the General Information section, in the Import Type drop-down list, select Create New Records.
9. In the Import Fields Mapping section, ensure that all the values in the Application Fields row match the column headers.
   Note: If a value does not match, click the drop-down list for the item, and select the appropriate value.
10. Click Next.
11. Ensure that the summary information from the Data Import Wizard is correct, and click Import.
12. Complete steps 1 to 11 again to import the Separated_Task.CSV that you created and saved earlier (Separate Incident Response Procedures and Tasks).
13. Manually link the Incident Response Procedures to the tasks.
    a. Click Edit for each incident response procedure in the Incident Response Procedure Library application.
    b. Click Lookup.
    c. Select the incident response tasks.
    d. Click OK.

Import Migrated Data into Incident Response Procedures Application

Procedure

1. Locate the CSV files you created and saved in ***Separate Incident Response Procedures and Tasks***, Separated_Procedures.CSV and Separated_Task.CSV.
2. In the Incident Response solution, in the Incident Response Procedure application, delete all previously existing records.
3. From the Navigation Menu, select Administration > Integration > Manage Data Imports.
4. In the Incident Response solution, in the Incident Response Procedures application, do one of the following:
    - If you are importing your incident response procedures, select the Incident Response Procedure level.
    - If you are importing your incident response tasks, select the Incident Response Task level.
5. In the Data Import Wizard, in the General Information section, select Browse.
6. From the File Upload window, click Add New.
7. Select the Procedures.CSV file that you created and saved earlier (Separate Incident Response Procedures and Tasks).

8. In the Format Options section, leave all the fields as default, and click Next.
9. From the General Information section, in the Import Type drop-down list, select Create New Records.
10. In the Import Field Mapping section, ensure that all of the values in the Application Fields row match the column headers.
    Note: If a value does not match, click the drop-down list for the item, and select the appropriate value.

11. Click Next.
12. Ensure that the summary information from the Data Import Wizard is correct, and click Import.
13. Complete steps 1 to 11 again to import the Task_Information.CSV that you created and saved earlier (Separate Incident Response Procedures and Tasks).
14. Manually link the Incident Response Tasks to the procedures.
    a. Click Edit for each incident response procedure in the Incident Response Procedure Library application.
    b. Click Lookup.
    c. Select the incident response tasks.
    d. Click OK.

Release 1.3 Service Pack 1 Patch 2

Fixed Issues

This section lists issues that were fixed in the current release.

Component	Tracking ID	Description
UCF	ARCHER-44175	Security Incident Management enhanced to support integration of the NetWitness 11.0 Respond module.

This section lists pertinent information about the Security Incident Management 1.3.1.2 release. **Note**: Although the official name of this release is Security Incident Management 1.3 SP1 P2, and the build number of this release is 1.3.1.53.26

Release Information	Description
Installer Name	RSA-Unified-Collector-Framework
Supported Paths (Upgrade/Install)	Upgrade from: version 1.3.1.1 Fresh install: version 1.3.1.2
Qualified Archer Versions	6.2. and 6.3
Qualified NetWitness Versions	11.0

Pre-requisites

There are installer changes in this release which require .NET 4 or later as a pre-requisite along with the existing pre-requisite requirements for the UCF install.

Upgrade guidelines

1. Please stop RSA Unified Collector Framework service and RSA SecOps Watchdog service, connectionmanager.bat or any open files prior to performing the upgrade.
2. Follow the steps through the installer.
3. Post the upgrade, and then restart the UCF windows server.
4. Make sure that the RSA Unified Collector Framework service and the RSA SecOps Watchdog service are running after the system restart.

NW 11.0 Integration

Please follow the instructions in the document at the link below to integrate NW 11.0 with Archer. Also, please look into the Known Issues section in the current document before you perform the integration.
Netwitness 11.0 and Archer Integration Guide

Known Issues

This section lists issues that were known at the time of the 1.3.1.2 release. Wherever a workaround or fix is available, it is noted or referenced in detail.

Component	Tracking ID	Description
UCF	ARCHER-44597	keystore.crt.pem generated by UCF contains an extra blank line that causes the orchestration command to deploy the UCF certificate on NetWitness server to fail: orchestration-cli-client --update-admin-node **Workaround:** Remove the blank line in keystore.crt.pem before performing the orchestration command.
RSA Archer Solution and NW 11.0	ASOC-41891	Investigation deep links from Archer to NetWitness Respond do not function. **Workaround:** Use the following URL instead : https://<NWServer Hostname or IP address>/respond/alert/<alert id>
NW 11.0	Not Applicable	Netwitness Respond 11.0 does not yet support Data Breach and Remediation task integration with Archer.

Release 1.3 Service Pack 1 Patch 1

Fixed Issues

This section lists issues that were fixed in the current release.

Component	Tracking ID	Description
Install/Upgrade	ARCHER-24676	Installer fix to include a missing visual C++ library causing a failure during the startup of the RSA Unified Collector Framework service on Windows 2012 R2.
UCF	ARCHER-24164	When logs are set to INFO level logging, the “CreateUserSessionFromInstance” soap call password is no longer shown in plain text.

Release Information1.3

RSA Archer Security Incident Management Release Notes release 1.0 and later

This section lists pertinent information about the Security Incident Management 1.3.1.1 release.

Note: Although the official name of this release is *Security Incident Management 1.3 SP1 P1*, the build number of this release is 1.3.1.52.58

Release Information	Description
Installer Name	RSA-Unified-Collector-Framework-1.3.1.52.58
Supported Paths (Upgrade/Install)	Upgrade from: • 1.3 • 1.3.1 Fresh Install: • 1.3.1.1
Qualified Archer Versions	6.1, 6.2, and 6.2.0.1
Qualified Security Analytics Versions	10.6.0.1 and 10.6.2.1

Release 1.3 Patch 1

Fixed Issues

This section lists issues that were fixed in the current release.

Component	Tracking ID	Description
RSA Archer Solution	ARCHCE-3554	Date/Time Closed and Davs Open fields are incorrectly updating during a recalculation job.
UCF	ARCHCE-3039	RSA Archer endpoint creation fails when an "&" exists in the API user password.
UCF	ARCHCE-3196	The Alert Name Encoded field from RSA Security Analytics is not being displayed in RSA Archer.
UCF	ARCHCE-3587	Alerts link to existing incidents, or create new incidents, based upon aggregation criteria if the message is coming through the Syslog channel.
UCF	ARCHCE-3807	Unrecognized characters in the Syslog payload were not allowing alerts to be processed.
UCF	ARCHCE-3840	Custom data from ArcSight is being appended to the Categ_Arcsight field in c6a4 format.
UCF	ARCHCE-3871	The UCF is now CEF v22 compliant.

Documentation Errata 1.3 Patch 1

This section includes corrections to the RSA Security Incident Management 1.3 SP1 documentation set.

Installation Options

You can apply the RSA Archer Security Incident Management 1.3 P1 changes in the following two ways:

- Option 1 - Update RSA Archer Security Incident Management 1.3 manually without installing the 1.3 P1 package.
- Option 2 - Standard installation.

Note: If the existing environment is customized, RSA recommends using Option 1 to manually apply the patch.

Installation Option One

Update RSA Archer Security Incident Management 1.3 manually without installing the 1.3 P1 package.

Procedure

1. Log in as System Administrator.
2. Go to Navigation Menu > Administration > Application Builder > Manage Applications > Security Alerts.
3. Click the Fields tab.
4. Update the ESA Severity field as follows:
    a. Select the ESA Severity field.
    b. Click Add New.
    c. In the Text Value field, enter Critical.
    d. Click Save.
    e. Click the Options tab.
    f. Delete the existing formula.
    g. Enter the following formula:

```
IF([Status]=VALUEOF([Status],"Closed"),[ESA Severity],IF
(OR([Helper ESA Severity Calc]="3",[Helper ESA Severity
Calc]="1"),VALUEOF([ESA Severity],"Low"),IF([Helper ESA
Severity Calc]="5",VALUEOF([ESA Severity],"Medium"),IF
([Helper ESA Severity Calc]="7",VALUEOF([ESA
Severity],"High"),IF([Helper ESA Severity
Calc]="9",VALUEOF([ESA Severity],"Critical"),NOVALUE
()))))))
```

    h. Click Validate.
    i. Click OK.
    j. Click Save.
5. Update the Security Alert Priority field formula as follows:
    a. Select the Security Alert Priority field.
    b. Click the Options tab.
    c. In the Calculate Properties section, click Edit Formula.
    d. Delete the existing formula.
    e. Enter the following formula:

```
IF([Source]=VALUEOF([Source],"Security Analytics
(Incident Management)"),NOVALUE(), IF(AND
([Source]=VALUEOF([Source],"Security Analytics (ESA)"),
[Status]=VALUEOF([Status],"Closed")),[Security Alert
Priority],IF ([Source]=VALUEOF([Source],"Security
Analytics (ESA)"),IF(OR([Helper ESA Severity Calc]="3",
[Helper ESA Severity Calc]="1"),VALUEOF ([Security Alert
Priority],"P-3"),IF([Helper ESA Severity
Calc]="5",VALUEOF([Security Alert Priority],"P-2"),IF
([Helper ESA Severity Calc]="7",VALUEOF([Security Alert
Priority],"P-1"),IF ([Helper ESA Severity
Calc]="9",VALUEOF([Security Alert Priority],"P-
0"),NOVALUE())))),IF(([Severity Level])<=2,VALUEOF
([Security Alert Priority],"P-3"),IF(([Severity
Level])<=5,VALUEOF([Security Alert Priority],"P-2"),IF
(([Severity Level])<=8,VALUEOF([Security Alert
Priority],"P-1"),IF(([Severity Level])<=10,VALUEOF
([Security Alert Priority],"P-0"))))))))
```

    f. Click Validate.
    g. Click OK.
    h. Click Save.
6. Update the Priority Values List in the Global Values List.

a. Go to Navigation Menu > Administration > Application Builder > Manage Global Values Lists.
b. Select GVL Priority.
c. Edit the values as follows:
   - Change the P3 to high, delete the image, click Save.
   - Change the P0 to Low, delete the image, click Save.
   - Change the P1 to Medium, delete the image, click Save.
   - Delete P2.
d. Click Save.

Note: DO not set default values.

7. Remove duplicate values from the States values list in the Global Values List.
   a. Select GVL:States.
   b. Delete the following values:

ID	NC	OH	CO	KS
MO	CA	OR	VA	FL
AZ	IL	TN	WA	NY
IA	OK	MN	NE	SD
TX	NM	WY	WI	ND
AR	MT	NV	UT	CT
PA	MA	ME	NH	DC
MD	RI	NJ	SC	WV
VT	DE	KY		

   c. Click Save.

.

Installation Option Two

Complete the standard installation of the RSA Archer Security Incident Management solution.

Procedure

Install the updated package. For more information, see Chapter 2, "Installing the RSA Archer Security Incident Management Solution," in the *RSA Archer Security Incident Management 1.3 Installation and Configuration Guide*.

Release 1.3

Fixed Issues

This section lists issues that were fixed in the 1.3 release.

Component	Tracking ID	Description
Install/ Upgrade	SOC-1360	During upgrade, the existing keystore.p12 file is replaced with the new keystore.
Splunk	SOC-1422	Alerts in RSA Archer GRC from Splunk are time stamped nine hours later than the original alert timestamp.
UCF	SOC-1341	When the RSA Archer GRC endpoint is configured successfully, there are some connection errors in the connection manager log.
UCF	SOC-1454	In RSA Security Analytics Incident Management (SA IM), if the incidents were created without association to a category, the RSA Unified Collector Framework (UCF) failed to process such incidents by throwing an exception.
UCF	SOC-1548	If the RSA Archer GRC URL does not have the context / virtual directory with the base URL, the connection between the UCF and RSA Archer GRC fails.

Known Issues

This section lists issues that were known at the time of the 1.3 release. Wherever a workaround or fix is available, it is noted or referenced in detail.

Component	Tracking ID	Description
Install/Upgrade, Migration	SOC-1612	When RCF migration for the Enterprise Management (EM) plug-in with SSL is performed, the certificates are not migrated, therefore the secure connection on the RSA Security Analytics (SA) host does not work. Workaround: After migration for EM Plug-in with SSL, regenerate the certificates and deploy the certificates automatically to the SA host. For more information,

		see "Regenerate Certificates" in the *RSA Archer Security Operations Management 1.3 SP1 Installation and Configuration Guide*.
UCF	SOC-1498	If the RSA Security Analytics Reporting Engine (SA RE) is configured in secure TCP mode and the certificates are not copied to the trust store, the connection still works.
UCF	SOC-1511	If a pre-configured RSA Security Analytics Incident Management (SA IM) endpoint is edited and the connection fails, or if there is an invalid configuration, the endpoint is not saved. Workaround: Delete and then re-add the SA IM endpoint.
UCF	SOC-1553	When RabbitMQ is down, the messages on the queue in RSA Archer Security Incident Management is lost when RabbitMQ connectivity returns.
UCF	SOC-1554	When RabbitMQ is down, updates to incidents from RSA Archer GRC to SA IM are not saved in the queue to be sent after the RabbitMQ connectivity returns.
UCF	SOC-1558	While using the Test Syslog Client from Connection Manager, if a drive is mentioned, such as C: or X:, then the connection manager closes with an exception. Workaround: Provide a folder with a file path, such as C:\test\, instead of a drive letter.
UCF	SOC-1604	If the RSA Archer GRC Web Server goes offline, the messages in the queue are not sent to RSA Archer GRC after the server comes online.

Release 1.2 Patch 2

Fixed Issues

This section lists issues that were fixed in the 1.2 P2 release

Component	Tracking ID	Description
Data Feeds	ARCHCE-1475	The Security Incident - Generate Incident Response Procedures and Tasks data feed manager duplicates the incident response tasks within same procedure when security incident threat category changes. To fix this issue, see ***Replace the RSA Archer Security Operations Management DFX5 File.***

Installing RSA Archer Security Incident Management 1.2 Patch 2

This patch must be installed on a machine that already had RSA Archer Security Incident Management 1.2 or RSA Archer Security Incident Management 1.2 P1 installed and fully functional.

The following software must be installed and fully functional before running the RSA Archer Security Incident Management patch installer:

- Java Runtime Environment (JRE) 7
- .NET Framework 3.5

The following files are included in the RSA_SecOps1.2_SP0_P2.zip file:

- RSA_Connector_Framework_Plugin.exe
- RSA_Unified_Collector_Framework.exe
- em_1.2.0.xxb4.zip

The following file is included in this release and is necessary for updating the data feed manager. It is contained in the RSA_Archer_Security_Operations_Management_1.2.zip file:

- RSA_Archer_Security_Operations_Management_1.2.0.2_Data_Feeds.zip

Install RSA Archer Security Incident Management Patch 1.2 P2

Procedure

1. On your SA IM Integration Service system, click Control Panel > Administrative Tools > Services.
2. Select RSA SA IM – Data Collector.
3. Click Stop.
4. Ensure that all files, folders, and prompt are closed.
5. Extract the RSA_SecOps1.2_SP0_P2.zip file to a local folder on your machine.
6. Double-click RSA_Unified_Collector_Framework.exe.
7. Click Next.

8. Read and accept the license agreement.
9. Click Next.
10. Select one or both:
    - RSA Connector Framework – necessary to integrate with third-party SIEM tools or to send business context data from your RSA Archer system to RSA Security Analytics.
    - SA IM Integration Services – necessary to integrate with RSA Security Analytics Incident Management.
11. To update the RSA Connector Framework, do the following:
    a. When prompted to update your installation, click Yes.
    b. Verify the plug-ins to update, and click Yes.
    c. Click Next.

       Note: The SecOps plug-in is used for integrating with third-party SIEM tools. The Enterprise Management (EM) plug-in is used to feed business context from the RSA Archer Enterprise Management solution into RSA Security Analytics.
    d. Click Finish.
12. To update the SA IM Integration Service, do the following:
    a. When prompted to update the SA IM Integration service, click Next.
    b. Read and accept the license agreement.
    c. Click Next.
    d. Click Install.
    e. Click Finish.
13. Update the data feed file from the RSA_Archer_Security_Operations_Management_1.2.0.2_Data_Feeds.zip

Release 1.2 Patch 1

Fixed Issues

This section lists issues that were fixed in the 1.2 P1 release

Component	Tracking ID	Description
RCF	SOC-1236	If the IP address of the device location where alerts are sent is changed in RSA Archer GRC, security alerts are linked to incorrect device records.
RCF	SOC1244	The RCF user Time Zone setting is not configured to UTC London/Dublin resulting in a difference of two hours between the alert timestamp and ESA. See ***Change the Time Zone of the RCF User Account.***
SA IM Integration Service	SOC-1243	If the IP address of the device location where alerts are sent is changed in RSA Archer GRC, security alerts are linked to incorrect device records.

Installing RSA Archer Security Incident Management 1.2 Patch 1

This patch must be installed on a machine that already has RSA Security Incident Management 1.2 installed and fully functional.

The following files are included in the RSA_SecOps1.2_SP0_xx.zip file:

- RSA_Connector_Framework_Plugin.exe
- RSA_Unified_Collector_Framework.exe
- em_1.2.0.xxb4.zip

Install RSA Archer Security Incident Management 1.2 Patch 1 Procedure

1. On your SA IM Integration Service system, click Control Panel > Administrative Tools > Services.
2. Select RSA SA IM – Data Collector.
3. Click Stop.
4. Ensure al files, folders, and prompts are closed.
5. Double-click RSA_Unified_Collector_Framework.exe.
6. Click Next.
7. Read and accept the license agreement.
8. Click Next.
9. Choose one or both:
    - RSA Connector Framework – necessary with third-party SIEM tools or to send business context data from your RSA Archer system to RSA Security Analytics.
    - SA IM Integrations Service – necessary to integrate with RSA Security Analytics Incident Management.
10. To update the RSA Connector Framework, do the following:
    a. When prompted to update your installation, click Yes.
    b. Verify the plug-ins to update, and click Next.
    c. Click Next.
    Note: The SecOps plug-in is used for integrating with third-party SIEM tools. The Enterprise Management (EM) plug-in is used to feed business context from the RSA Archer Enterprise Management solution into RSA Security Analytics.
    d. Click Finish.
11. To update the SA IM Integration Service, do the following:
    a. When prompted to update the SA IM Integration service, click Next.
    b. Read and accept the license agreement.
    c. Click Next.
    d. Click Install.
    e. Click Finish.

Space Requirements for the RSA Connector Framework

The RSA Connector Framework (RCF) is required in RSA Archer Security Incident Management 1.2 to carry the business context information from RSA Archer GRC to RSA Security Analytics. The RCF requires less hard drive space in this release. Alerts generated from the RSA Security Analytics Incident Management (SA IM) module are communicated through the SA IM Integration Service and not through the RCF.

Install the RSA Archer Enterprise Management Plug-in

If you did not install the RSA Archer Enterprise Management plug-in when you installed the RCF, you can install the plug-in separately.

Note: Only plug-ins that are located in the same folder as the RSA_Connector_ Framework_Plugin.exe file can be installed. Ensure that the plug-in you want to install is in this folder.

Procedure

1. Double-click the RSA_Connector_Framework_Plugin.exe.
2. Click Next.
3. Read and accept the license agreement.
4. Click Next.
5. Select the plugin that you want to install.
6. Click Next.
7. Click Install.
8. Click Finish.

Change the Time Zone of the RCF User Account

Procedure

1. Go to Administration > Access Control > Manage Users.
2. Select the RCF user account.
3. In the Localization section, set the time zone to (UTC) Dublin, Edinburgh, Lisbon, London.
4. Click Save.

Release 1.2

Known Issues

This section lists issues that were known at the time of the 1.2 release. Wherever a workaround or fix is available, it is noted or referenced in detail.

Component	Tracking ID	Description
Incident Management subsolution	SOC-416	After installation, only the key field is displayed in the grid for the Business Unit field and the Facilities field. You must configure additional fields to display in the grid for each field. Note: This issue exists only in RSA Archer Platform 5.5. Workaround: 1. Navigate to the field in which you want to update the grid display. 2. Select the Options tab. 3. In the Grid Display Properties section, select which fields from a related application will display when a user selects this option. 4. Click OK. 5. Click Save.
Incident Management subsolution	SOC-1186	After installation of the Security Alert Priority field is displayed on the Alerts tab of an incident received from Security Analytics Incident Management. Workaround: 1. Click Administration > Application Builder > Manage Applications. 2. Click Security Incidents and click the Fields tab. 3. Click Security Alerts and click the Options tab. 4. In the Display Fields field, click […]. 5. Remove Security Alert Priority and click OK. 6. Save the field. 7. Save the application.
SA IM Integration Service Setup	SOC-1190	When using the SA IM Integration Service to

		communicate with Security Analytics over SSL on a Windows Server 2008 R2 Enterprise edition machine, a "connection reset" error occurs for four to five minutes before a successful connection is found. This occurs at every restart of the service. Workaround: Wait four to five minutes for the service to connect.
RSA Archer Platform	SOC-474	Users with Read Only access to the RSA Archer Enterprise Management solution are unable to see the Information Assets application. **Note:** This issue exists only in RSA Archer Platform 5.5. Workaround: Manually assign users with EM Read Only access. For instructions, see “Assign an Access Role to a User” or “Assign a User Group to an Access Role” in the RSA Archer Help.
SOC Management subsolution	SOC-457	When you create and save a Degrees and Certifications record from a Contacts record, an error message may appear that reads "The content in field Training Courses (Education) violates the required rule established in the related field." Workaround: Click OK. The cross-referenced Degrees and Certifications record is saved and displays as expected.

Release 1.1

Fixed Issues

This section lists issues that were fixed in the 1.1 release.

Component	Tracking ID	Description
Breach Management	SOC-476	The SOC:Business Manager, SOC:HR, SOC:Legal, and SOC:Compliance/Privacy Officer access roles did not have access to the Breach Risk Assessment questionnaire and, as a result, users assigned these roles were unable to see questionnaires.
Dashboards and Workspaces	SOC-400	In the Security Tools Efficacy iView, in the SOC Manager dashboard, HTML tags displayed instead of white space between text.
Incident Management	SOC-473	In the Incident Investigations application, in the Remediation tab, selecting No in the Remediation Required field hid all of the other related fields.
Incident Management	SOC-477	Users assigned the SOC:Business Manager access role could see the Security Alerts application in the left navigation menu even though they did not have access to any records in the application.
Issue Management	SOC-470	Users with access to a Data Breaches or Incident Investigations record could only view related Findings records that they created or to which they are assigned. Users are now able to see all related Findings records.
Reports Dashboard	SOC-471	The Number of Investigations by Priority report, in the All Queues by Priority iView, displayed only new investigations. The report now includes all investigations except those that are resolved.

Known Issues

This section lists issues that were known at the time of the 1.1 release. Wherever a workaround or fix is available, it is noted or referenced in detail.

Component	Tracking ID	Description
Incident Management	SOC-416	After installation, only the key

subsolution		field is displayed in the grid for the Business Unit field and the Facilities field. You must configure additional fields to display in the grid for each field. **Note:** This issue exists only in RSA Archer Platform 5.5. Workaround: 1. Navigate to the field in which you want to upgrade the grid display. 2. Select the Options tab. 3. In the Grid Display Properties section, select which fields from a related application will display when a user selects this option. 4. Click OK. 5. Click Save.
RSA Archer Platform	SOC-474	Users with Read Only access to the RSA Archer Enterprise Management solution are unable to see the Information Assets application. Workaround: Manually assign users with EM Read Only access. For instructions, see "Assign an Access Role to a User" or "Assign a User Group to an Access Role" in the RSA Archer Help.
SOC Management subsolution	SOC-457	When you create and save a Degrees and Certifications record from a Contacts record, an error message may appear that reads "The content in field Training Courses (Education) violates the required rule established in the related field." Workaround: Click OK. The cross-referenced Degrees and Certifications record is saved and displays as expected.

Release 1.0

Known Issues

This section lists issues that were known at the time of the 1.0 release. Wherever a workaround or fix is available, it is noted or referenced in detail.

<table>
<tr><th>Component</th><th>Tracking ID</th><th>Description</th></tr>
<tr><td>iView</td><td>SOC-400</td><td>In the Security Tools Efficacy iView, in the SOC Manager dashboard, HTML tags display instead of white space between text. Currently, there is no workaround for this issue.</td></tr>
<tr><td>Records</td><td>SOC-457</td><td>When you create and save a Degrees and Certifications record from a Contacts record, an error message may appear that reads “The content in field Training Courses (Education) violates the required rule established in the related field.”

Workaround:

Click OK. The cross-reference Degrees and Certifications record is saved and displays as expected.</td></tr>
<tr><td>Records</td><td>SOC-470</td><td>Users who have access to a Data Breaches or Incident Investigations record can only view related Findings records that they created or to which they are assigned. Users should be able to see all related Findings records.

Workaround:

1. Click Administration > Application Builder > Manage Applications.
2. Select Findings.
3. Click the Fields tab.
4. Click Inherited Record Permissions.
5. Click the Options tab.
6. In the Field Population section, add the following:
<table>
<tr><th>Application</th><th>Users</th></tr>
<tr><td>Data Breaches</td><td>• Breach Response Lead
• Business Manager
• Compliance/Privacy Officer
• Customer Support
• IT Manager
• Legal Analyst
• Other Members
• Public Relations</td></tr>
<tr><td>Incident Investigations</td><td>• Business Manager
• Compliance Officer
• HR Analyst</td></tr>
</table>
</td></tr>
</table>

		• Investigation Coordinator • Investigation Owner • Legal Counsel • Other Members 7. Save the field and the application.
Records	SOC-471	The Number of Investigations by Priority report, in the All Queues by Priority iView, displays only new investigations. The report should include all investigations except those that are resolved. Workaround: 1. In the Navigation menu, expand Incident Investigations > Reports. 2. Select Number of Investigations by Priority. 3. Click Modify. 4. In the Filters section, for the first filter, change the Operator field to Does Not Contain and the Value(s) field to Resolve. 5. Click Search. 6. Click Save.
Reports	SOC-473	In the Incident Investigations application, in the Remediation tab, when you select No in the Remediation Required field, all of the other fields are hidden. If you previously selected Yes and created Findings records, these records still exist yet are no longer visible or accessible through the Investigation record. Workaround: 1. Click Administration > Application Builder, Manage Applications. 2. Select Incident Investigations. 3. Click the Events tab. 4. Click the Hide_Specify_Remediation_Action rule. 5. In the Status field, select Inactive. 6. Save the rule and the application.
Access Roles	SOC-476	The SOC:Business Manager, SOC:HR, SOC:Legal, and SOC:Compliance/Privacy Officer access roles are missing access to the Breach Risk Assessment questionnaire and, as a result, users assigned these roles are unable to see questionnaires. Workaround: Update the affected access role to provide correct access. 1. Click Administration > Access Control > Manage Access Roles. 2. Select SOC: Business Manager. 3. Click the Rights tab.

<table>
<tr>
<td></td>
<td></td>
<td>
4. In the Application column, filter by Breach Risk Assessment.
5. Assign the following rights:
<table>
<tr><th>Page Type</th><th>Rights</th></tr>
<tr><td>Content Record</td><td>Create, Read, Update</td></tr>
<tr><td>Data Import</td><td>Create, Read, Update</td></tr>
<tr><td>Email Option</td><td>Read</td></tr>
<tr><td>Export Option</td><td>Read</td></tr>
<tr><td>Print Option</td><td>Read</td></tr>
<tr><td>Save Report</td><td>Create, Read, Update</td></tr>
</table>
6. Click Save.
7. Repeat steps 2-6 for the HR, Legal, and Compliance/Privacy Officer access roles.
</td>
</tr>
<tr>
<td>Application</td>
<td>SOC-477</td>
<td>
Users assigned the SOC:Business Manager access role can see the Security Alerts application in the left navigation menu, even though they do not have access to any records in the application.

Workaround: Update the Business Manager access role.

1. Click Administration > Access Control > Manage Access Roles.
2. Select SOC:Business Manager.
3. Click the Rights tab.
4. In the Application column, filter by Security Alerts.
5. In the Content Record row, clear the Read checkbox.
6. Click Save.
</td>
</tr>
</table>