RSA Archer GRC

RSA Archer Security Operations Management 1.3

Release Notes

5.4 SP1 or 5.5, 5.5 SP1, 5.5 SP2, and 5.5 SP3

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers:
http://www.emc.com/support/rsa/index.htm.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, 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 EMC.

Third-party licenses

This product may include software developed by parties other than RSA.

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.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION 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 2015

Contents

Preface

This document lists what's new and changed in RSA® Archer® Security Operations Management.

These *Release Notes* may be updated. The most current version can be found on RSA SecurCare® Online at **https://knowledge.rsasecurity.com**.

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

Support and Service

Customer Support Information	**www.emc.com/support/rsa/index.htm**
Customer Support E-mail	**archersupport@rsa.com**

Other Resources

RSA Archer Community enables collaboration among GRC clients, partners, and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide the RSA Archer GRC product roadmap.
https://community.emc.com/community/connect/grc_ecosystem/rsa_archer

RSA Archer Exchange is an online marketplace dedicated to supporting GRC initiatives that delivers on-demand applications with service, content, and integration providers to drive the success of RSA Archer GRC clients.
https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange

RSA Solution Gallery provides information about third-party hardware and software products that have been certified to work with RSA products. The gallery includes Secured by RSA Implementation Guides with instructions and other information about interoperation of RSA products with these third-party products.
https://gallery.emc.com/community/marketplace/

RSA SecurCare Online (SCOL) provides unlimited access to a wealth of resources on the Web, 24 hours a day. The secure system provides members access to a support knowledgebase, to download current platform patches and bug fixes, to sign up for notifications, to manage your support cases and more.
https://knowledge.rsasecurity.com/

RSA Archer GRC Documentation

You can access the RSA Archer GRC documentation from the RSA Archer Exchange and RSA Archer Community.

Documentation	Location
Platform	On the RSA Archer Community at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer**
Solutions, Applications, and Content	On Content tab on the RSA Archer Exchange at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange**

RSA continues to assess and improve the documentation. Check the RSA Archer Community and RSA Archer Exchange for the latest documentation.

RSA Archer Security Operations Management Release 1.3

What's New in Release 1.3

Component	Description
Middleware Monitoring	The RSA SecOps Watchdog Service tracks and reports the number of messages read from RabbitMQ or Syslog servers, and the number of messages that have been created or updated in RSA Archer GRC. The RSA SecOps Watchdog Service is responsible for reading all of the counters from the Windows Performance Counters at every Configured Cron Time, logging the appropriate messages, and performing any actions deemed necessary.

SIEM Tools	The following SIEM tools are now supported out of the box:
	• RSA Security Analytics 10.4 and 10.5
	  • RSA Security Analytics Incident Management
	  • RSA Security Analytics Reporting Engine
	  • RSA Security Analytics Event Stream Analysis
	• HP ArcSight 5.0 SP1
	• Splunk Enterprise 6.2.4
	• McAfee Enterprise Security Manager 9.5.0
	• IBM QRadar 7.2.5
	Generic SIEM tools supporting Syslog can be configured in the RSA Unified Collector Framework. For more information, see the *RSA Archer Security Operations Management 1.3 Installation and Configuration Guide*.

SA IM Integration Service	The RSA Security Analytics Incident Management (SA IM) Integration Service functionality is now part of the RSA Unified Collector Framework (UCF).

Component	Description
UCF	RSA Archer Security Operations Management uses the RSA Unified Collector Framework (UCF) instead of the RSA Connector Framework (RCF) for easier integration. All RCF functionality has been moved to the UCF.
UCF	Through the new migration feature, customized mapping files from previous versions of RSA Archer Security Operations Management can be migrated into RSA Archer Security Operations Management 1.3.
UCF	Certificates are now automatically generated during integration, eliminating the need to enter SSL commands to generate certificates. Once configuration is complete, you are notified about whether the certificates were successfully verified.
UCF	JRE 1.8 is now supported.

Fixed Issues in Release 1.3

The following issues were fixed in the current 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 timestamped 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 in Release 1.3

This section lists reported issues that remain unresolved as of the latest release. Wherever a workaround or fix is available, it is noted or referenced in detail. For many of the issues in this section, you must have administrative privileges.

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 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 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 Operations Management are 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

Component	Tracking ID	Description
		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.