

ServiceNow ITSM Integration



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

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.

February 2018

Contents

Se	rviceNow ITSM Integration with RSA NetWitness	4
	Prerequisites	4
	Integration Steps	4
	Install the RSA NetWitness Incident Management Integration Application	4
	Configure RSA NetWitness Incident Notifications	5

ServiceNow ITSM Integration with RSA NetWitness

The RSA NetWitness Suite Incidents module collects alerts from multiple sources and provides the ability to group them logically. You can then implement an Incident response workflow to investigate and remediate the security issues raised. If an alert matches a rule, an incident is created using the criteria. Customers who wants to use ServiceNow for centralized incident management can leverage this integration to send incidents from RSA NetWitness to a ServiceNow instance.

ServiceNow is a software platform that supports IT service management and automates common business processes. This software as a service (SaaS) platform contains a number of modular applications that can vary by instance and user. The RSA NetWitness integration with ServiceNow creates incidents in ServiceNow ITSM, based on email notifications received from RSA NetWitness Incident Management.

Prerequisites

For the integration, you need the following:

- Access to a ServiceNow instance
- RSA Security Analytics / NetWitness version 10.4.x or later

Integration Steps

There are two steps for integrating RSA NetWitness with ServiceNow:

- 1. Install the RSA NetWitness Incident Management Integration Application
- 2. Configure RSA NetWitness Incident Notifications

Install the RSA NetWitness Incident Management Integration

Application

1. Browse to the ServiceNow store and Search for **RSA Security Analytics IM** Integration application. The application appears in the Application list on the ServiceNow store as shown here:

service	ისw Store	Search	Q		Events Help - Log In
Home > Search Res	ults > RSA Security Analytics IM Integration				
RSΛ	RSA Security Analytics I Create ITSM Incidents based on email not by RSA Security LLC Compatibility: Jakarta	M Integration ification from RSA Security Analyt	ics Incident Managemen	t.	Get Pricing Free
습습습습습 N	o Reviews			Share 🔽 📻	Compatibility

2. Click Get.

After a successful installation of this application, the Administrator should be able to view the application under **Inbound Actions** in the ServiceNow instance.



Note: Make sure that email receiving is enabled on the ServiceNow instance, and disable the default **Create Incident** inbound action to avoid duplicate incidents.

Configure RSA NetWitness Incident Notifications

- 1. In the Security Analytics menu, select Incidents > Configure.
- 2. Click the **Notifications** tab.

Notification Settings Email Server Test Email Server Email Server Email Server Settings SOC Managers Workflow Incident Assignee? SOC Managers? Additional Addresses Template Incident is created Incident record is updated Incident status is changed Incident assignee is changed Incident category is changed Incident category is changed Incident task is created Incident task is updated Incident	Aggregation Rules Notifi	cations Int	egration	Retention Sch	eduler					
Email Server Test Email Server Email Server Email Server Settings SOC Managers Incident Assignee? SOC Managers? Additional Addresses Template Incident is created Incident record is updated Incident status is changed Incident status is changed Incident category is changed Incident task is created Incident task is updated	Notification Settings									
Email Server Settings SOC Managers Workflow Incident Assignee? Model is created Incident assignee? Incident is created Imagers? Incident record is updated Imagers? Incident status is changed Imagers? Incident assignee is changed Imagers? Incident assignee is changed Imagers? Incident assignee is changed Imagers? Incident category is changed Imagers? Remediation task is created Imagers? Remediation task is updated Imagers? Remediation task is closed Imagers?	Email Server	Test Email Ser	imail Server 🗸							
SOC Managers Incident Assignee? SOC Managers? Additional Addresses Template Incident is created Incident is created Image: Social Stream Stre		Email Server Se	l Server Settings							
Workflow Incident Assignee? SOC Managers? Additional Addresses Template Incident is created	SOC Managers	OC Managers								
Incident is created Implementation Implementation Incident record is updated Implementation Implementation Incident status is changed Implementation Implementation Incident assignee is changed Implementation Implementation Incident category is changed Implementation Implementation Remediation task is created Implementation Implementation Remediation task is closed Implementation Implementation Implementation task is closed Implementation Implementation	Workflow	Incide	nt Assignee?	SOC Managers?	Additional Addresses		Template			
Incident record is updated Incident status is changed Incident status is changed Incident assignee is changed Incident priority is changed Incident category is changed Incident category is changed Incident category is changed Remediation task is created Incident Remediation task is cosed Incident Remediation task is closed Incident	Incident is created						🗹 Edit			
Incident status is changed Incident assignee is changed Incident priority is changed Incident priority is changed Incident category is changed Incident category is changed Incident category is changed Incident category is changed Remediation task is created Incident category is changed Remediation task is updated Incident category is changed Incident category is changed Incident category is changed Incident category is changed Incident category is changed Remediation task is updated Incident category is changed Incident category is changed Incitry is changed <	Incident record is updated						🗹 Edit			
Incident assignee is changed	Incident status is change	ed								
Incident priority is changed Incident category is changed Incident category is changed Remediation task is created Remediation task is updated C Edit Remediation task is closed C Edit	Incident assignee is char	nged								
Incident category is changed Incident category is changed Remediation task is created Incident category is changed Incident category	Incident priority is chang	ged								
Remediation task is created Image: Constraint of task is updated Remediation task is updated Image: Constraint of task	Incident category is char	nged								
Remediation task is updated Image: Constraint of task is closed Image: Constraint of task o	Remediation task is created						🗹 Edit			
Remediation task is closed	Remediation task is updated						🗹 Edit			
4	Remediation task is closed						🗹 Edit			
	•						•			
	Арріу									
Арріу										

- 3. In the **SOC Managers** field, enter the email address for the ServiceNow instance email. For example, **Test12444@service-now.com**).
- 4. For the Incident is created workflow, click the Edit button to open the Template dialog box.
- 5. In the **Subject** field, enter the following text for the subject:

RSA Security Analytics IM Incident Created: (\${id}) \${name}



6. Locate the tag near the end of the template, and insert the following lines:

Incident Link :

\${incidentLink}



- 7. Click Save, to save your changes and close the dialog box.
- 8. Click **Apply** in the Notifications tab.

For more information on how to configure Incident Management, see Incident Management: Configure Notification Settings.

This completes the configuration.