RSA NETWITNESS®
SUITE

Release Notes

for Version 11.0.0.1

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

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. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. 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.

Distribution

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

Contents

Introduction

This document lists enhancements and fixes in RSA NetWitness Suite 11.0.0.1. Read this document before deploying or updating RSA NetWitness Suite 11.0.0.1.

- What’s New
- Fixed Issues
- Update Instructions
- Product Documentation
- Contacting Customer Care
- Revision History

What's New

RSA NetWitness Suite 11.0.0.1 patch provides additional security controls and fixes to 11.0.0.0. Following are the security controls and fixes included in this release.

Investigate

This patch enables additional security controls for NetWitness Investigate workflows, allowing further flexibility for administrators to apply user attributes that override role-based access (RBAC). By default, these security controls are not applied to the system but administrators have the option to restrict analysts from viewing data they do not have permission to view. The main changes related to Investigate are outlined below.

Role and User Attributes

The user attributes that were present in NetWitness 10.6.x and absent in NetWitness 11.0.0.0 are now available in this patch. The role attributes are already present in 11.0.0.0. Both are configurable in the **ADMIN** > **Security** view. The user attributes override the role attributes when applied. Both user and role attributes consist of three attributes: query prefix, session timeout, and query threshold. The attributes restrict user queries from Investigate. The query prefix is a way for an administrator to restrict access to the data a user is querying, based on the user permissions or role permissions.

Event Analysis Attributes

If there is a need to restrict access to data a user is querying, additional steps are necessary as NetWitness Suite 11.0.0.0 does not enforce user and role attributes in the new Investigate Event Analysis workflows, regardless of what is configured for role and user attributes. To restrict access to data, perform the steps described in "Post-Update Tasks" in the Update Instructions topic.

Active Directory Users

This patch addresses external user logins using Active Directory in 11.0.0.0. In a few cases, external users using Active Directory in Security Analytics release 10.6.4.1 or earlier were not able to log in to NetWitness 11.0.0.0. UI after the upgrade.

It is recommended that you do one of the following to address this issue:

- Apply the 10.6.4.2 patch before you upgrade to 11.0.0.0.
- If for some reason, the 10.6.4.2 patch is not applied, apply the 11.0.0.1 patch and then perform the External Authentication Migration.

Note: If you perform the External Authentication Migration, before applying the 10.6.4.2 or 11.0.0.1 patch, the external users will not be able to log in. Please contact RSA Customer Support to fix this issue.

User Logins

This patch addresses the user login issues in 11.0.0.0. Users cannot login to NetWitness Suite UI on installation of 11.0.0.0 or upgrade to 11.0.0.0. This is because the user interface cannot retrieve user account information from MongoDB. You must apply RSA NetWitness Suite 11.0.0.1 patch as soon as the installation of 11.0.0.0 or upgrade to 11.0.0.0 is completed.

Fixed Issues

This section lists issues fixed since the last major release.

Tracking Number	Description
ASOC-42734	If you configured user or role attributes to restrict access to data through query prefix in 10.6.4.x, and upgrade to 11.0, it does not work.
ASOC-42735	NetWitness Suite 11.0.0.0 does not enforce user and role attributes in the new Investigate Event Analysis workflows. If there is a need to restrict access to data a user is querying, regardless of what is configured for role and user attributes, you must lock down access as described in "Post-Update Tasks" in the Update Instructions topic.
ASOC-42738	If you have Active Directory users configured for external user logins in 10.6.4.1 or earlier, and upgrade to 11.0.0.0, these users will no be able to log in to NetWitness Suite UI.
ASOC-43523	Users cannot log in to NetWitness Suite UI on installation of 11.0.0.0 or upgrade to 11.0.0.0. This is because the user interface cannot retrieve user account information from MongoDB.

Update Instructions

You need to read the information and follow these procedures for updating RSA NetWitness Suite from version 11.0.0.0 to version 11.0.0.1.

The following update path is supported for RSA NetWitness Suite 11.0.0.1:

- RSA NetWitness Suite 11.0.0.0 to 11.0.0.1

Note: The 11.0.0.1 patch only applies to the NetWitness Server host.

You can update 11.0.0.1 patch using one of the following options:

- If the NetWitness Server has internet connectivity to SMC Update, the NetWitness Suite UI can be used to apply the patch.
- If the NetWitness Server does not have internet connectivity to SMC Update, the Command Line Interface (CLI) can be used to apply the patch.

Update Tasks

You can choose one of the following update methods based on your internet connectivity.

Online Method (Connectivity to SMC Update): Update using NetWitness UI

You can use this method if the NetWitness Server is connected to SMC Update and can obtain the package.

Note: If the NetWitness Server does not have access to SMC Update, use Offline Method (No connectivity to SMC Update): Update using the Command Line Interface .

Prerequisites

Make sure that:

1. The “Automatically download information about new updates every day” option is checked and is applied in **ADMIN** > **System** > **Updates** page.
2. 11.0.0.1 is available by clicking **ADMIN** > **Hosts** > **Update** > **Check for Updates**.
3. Host page displays the **Update Available** status.
4. 11.0.0.1 is available under “Update Version” column.

Procedure

1. Go to **ADMIN** > **Hosts**.
2. Select the NetWitness Server (nw-server) host.
3. Select **Update**.

4. Click **Update Host**.

5. Click the **Reboot Host** and restart the host.

Offline Method (No connectivity to SMC Update): Update using the Command Line Interface

You can use this method if the NetWitness Server is not connected to SMC Update.

Prerequisites

Make sure that:

- You have downloaded the below file, which contain all the NetWitness Suite 11.0.0.1 update files, from RSA Link (https://community.rsa.com/) > NetWitness Suite > RSA NetWitness Logs and Packets Downloads to a local directory:
  `netwitness-11.0.0.1.zip`

Procedure

1. Stage 11.0.0.1 by creating a directory on the NetWitness Server at `/tmp/upgrade/11.0.0.1` and extract the zip package.

2. Initialize the update on the NetWitness Server, using the following command:
   ```
   upgrade-cli-client --init --version 11.0.0.1 --stage-dir /tmp/upgrade
   ```

3. Update NetWitness Server, using the following command:
   ```
   upgrade-cli-client --upgrade--host-addr <IP of Netwitness Server> --version 11.0.0.1
   ```

> **Note:** The patch only applies to the NetWitness Server.

> **Note:** You can check versions of all the hosts, using the command `upgrade-cli-client --list` on NetWitness Server. If you want to view the help content of `upgrade-cli-client`, use the command `upgrade-cli-client --help`.

Post-Update Tasks

As the new Investigate Event Analysis does not enforce user and role attributes, you must lock down access to the Event Analysis workflow so users cannot bypass permission attributes:

1. Go to **ADMIN** > **Security**.

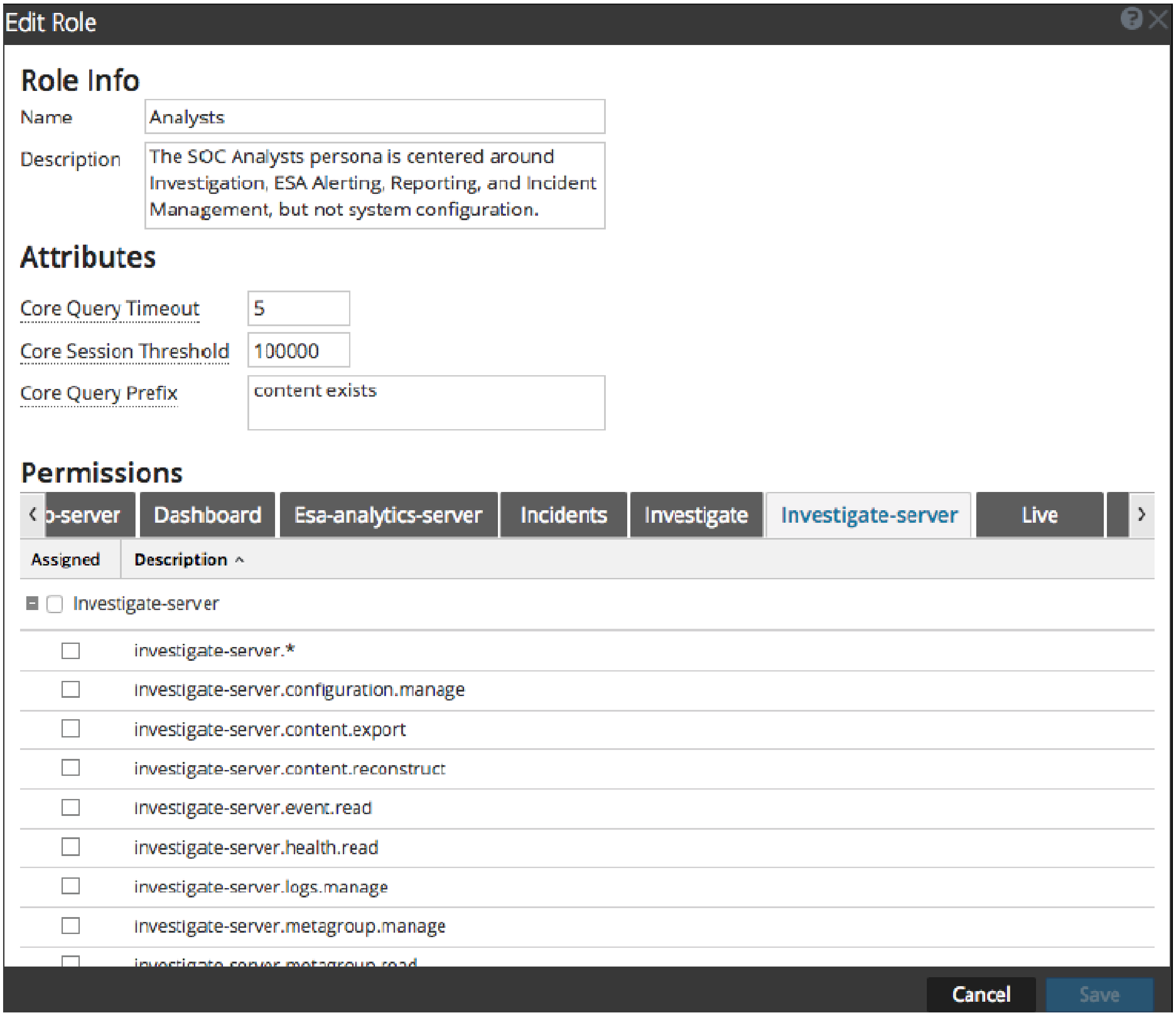
2. Select **Roles** tab.

3. Select a role and click ✎.

4. Select the **Investigate-server** tab.

5. Clear the **investigate-server*** checkbox.

> **Note:** By default, this checkbox is selected on update.



Role Info

Name: Analysts

Description: The SOC Analysts persona is centered around Investigation, ESA Alerting, Reporting, and Incident Management, but not system configuration.

Attributes

Core Query Timeout: 5

Core Session Threshold: 100000

Core Query Prefix: content exists

Permissions

Assigned	Description ^
□	Investigate-server
□	investigate-server.*
□	investigate-server.configuration.manage
□	investigate-server.content.export
□	investigate-server.content.reconstruct
□	investigate-server.event.read
□	investigate-server.health.read
□	investigate-server.logs.manage
□	investigate-server.metagroup.manage
□	investigate-server.metagroup.read

The following three access permissions have been added to allow further access control to the Event Analysis.

- **investigate-server.event.rea** provides access to meta, meta panel, and events list in Event Analysis.
- **investigate-server.content.export** provides access to downloads of files, PCAPs, logs, or endpoint events in Event Analysis.
- **investigate-server.content.reconstruct** provides access to packet analysis, text analysis, and file analysis views in Event Analysis.

- If you are not using user or role attributes, select all the three permissions to provide normal access.

- If you are using user or role attributes to restrict access to what users can view and want to limit all access to the Event Analysis, make sure these three and **investigate-server.*** permissions are not selected for each role the user is in.

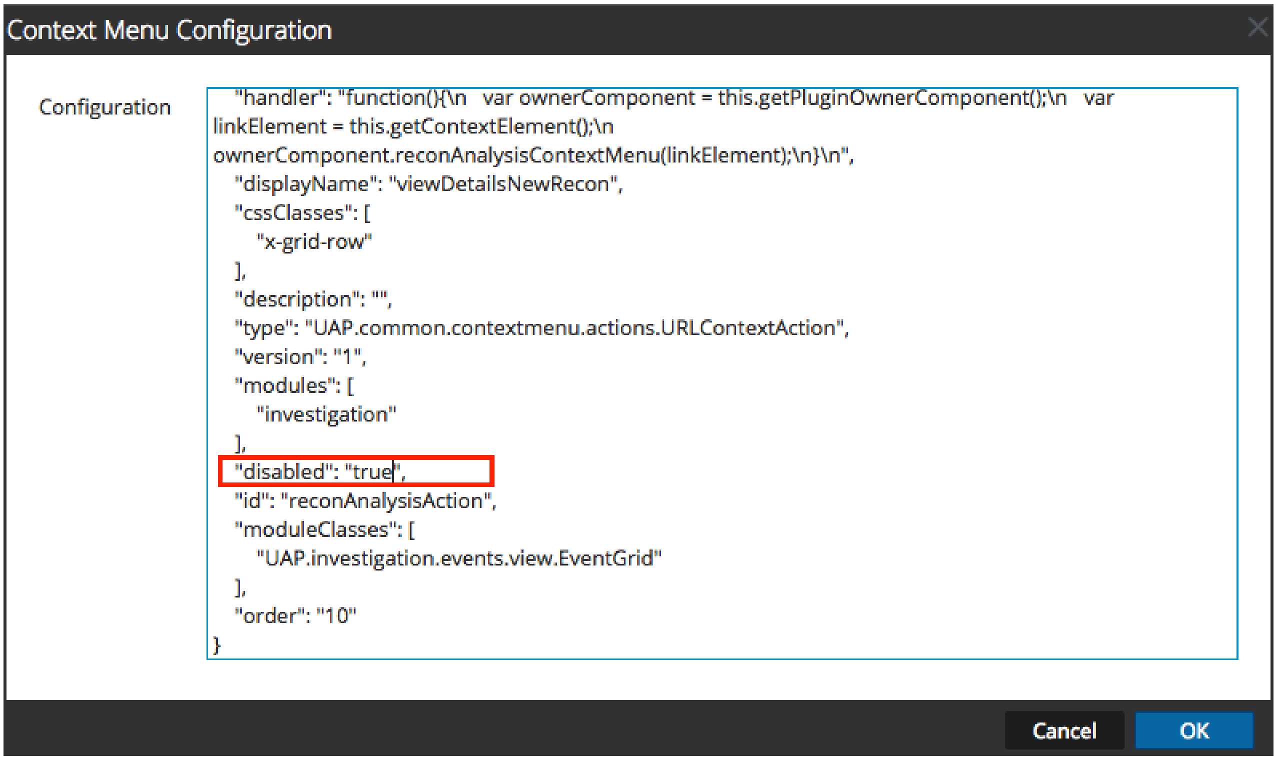
> **Note:** By default, the new permissions are not selected for all roles. These permissions will not be applied even if selected unless the investigate-server.* permission is disabled.

6. Click **Save**.

To lock down access to the Context Menu Action on Event Analysis, which is enabled by default, do the following:

1. Navigate to **ADMIN** > **System.**
2. Select **Context Menu Actions** from the left panel.
3. Select **Event Analysis**, and click ✎.

   The Context Menu Configuration dialog is displayed.



Context Menu Configuration

Configuration

```
   "handler": "function(){\n   var ownerComponent = this.getPluginOwnerComponent();\n   var
linkElement = this.getContextElement();\n
ownerComponent.reconAnalysisContextMenu(linkElement);\n}\n",
   "displayName": "viewDetailsNewRecon",
   "cssClasses": [
      "x-grid-row"
   ],
   "description": "",
   "type": "UAP.common.contextmenu.actions.URLContextAction",
   "version": "1",
   "modules": [
      "investigation"
   ],
   "disabled": "true",
   "id": "reconAnalysisAction",
   "moduleClasses": [
      "UAP.investigation.events.view.EventGrid"
   ],
   "order": "10"
}
```

4. Edit the disabled parameter and set it to "True".
5. Click **OK**.

Product Documentation

The following documentation is provided with this release.

Document	Location
RSA NetWitness Suite 11.0.0.0 Online Documentation	https://community.rsa.com/community/products/netwitness/110
RSA NetWitness Suite 11.0.0.0 Upgrade Instructions	https://community.rsa.com/community/products/netwitness/110
RSA NetWitness Suite 11.0.0.0 Upgrade Checklist	https://community.rsa.com/community/products/netwitness/110
RSA NetWitness Suite Hardware Setup Guides	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA Content for RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/rsa-content

Contacting Customer Care

Use the following contact information if you have any questions or need assistance.

RSA SecurCare	https://knowledge.rsasecurity.com
Phone	1-800-995-5095, option 3
International Contacts	http://www.emc.com/support/rsa/contact/phone-numbers.htm
Email	nwsupport@rsa.com
Community	https://community.rsa.com/docs/DOC-1294
Basic Support	Technical Support for your technical issues is available from 8 AM to 5 PM your local time, Monday through Friday.
Enhanced Support	Technical Support is available by phone 24 x 7 x 365 for Severity 1 and Severity 2 issues only.

Preparing to Contact Customer Care

When you contact Customer Care, you should be at your computer. Be prepared to give the following information:

- The version number of the RSA NetWitness Suite product or application you are using.
- The type of hardware you are using.

Revision History

Revision	Date	Description
1.0	25th October, 2017	GA