



# RSA Archer Integration Guide

for Version 11.0



## **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](http://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.

February 2018

# Contents

---

<b>RSA Archer Integration .....</b>	<b>4</b>
<b>Configure NetWitness to Work With Archer .....</b>	<b>5</b>
Create RSA Archer User Accounts for Push and Pull .....	5
Integrate NetWitness Suite With Archer SecOps Manager .....	7
RSA Unified Collector Framework (UCF) .....	7
Configure Respond for Integration with Archer SecOps .....	8
Configure Endpoints in RSA Unified Collector Framework .....	11
Configure Reporting Engine for Integration with NetWitness SecOps Manager .....	14
Configure Event Stream Analysis for Integration with Archer SecOps .....	16
RSA Archer Feeds .....	19
<b>Manage Unified Collector Framework .....</b>	<b>23</b>
<b>Troubleshoot RSA Archer Integration .....</b>	<b>24</b>
Setting the CA Truststore .....	24
Remediation Tasks in RSA Archer Security Operations Manager .....	24
Errors between RSA NetWitness Suite and RSA Unified Collector Framework .....	24

## RSA Archer Integration

Administrators can integrate RSA NetWitness Suite with RSA NetWitness Security Operations (SecOps) Manager to send alerts and incidents from NetWitness Suite to Archer for incident management and remediation. This guide provides a high-level workflow for configuring this integration.

**Note:** When you upgrade from Security Analytics 10.6.4 to NetWitness Suite 11.0, the Archer SecOps integration is no longer valid and must be re-configured.

The following table lists the NetWitness Suite 11.0 integration options with NetWitness SecOps Manager Version 1.3.1.2.

NetWitness SecOps Manager Version	NetWitness Suite 11.0 Integration	Reference
1.3.1.2	Event Stream Analysis (ESA)	For more information, see "Configure Event Stream Analysis for Integration with Archer SecOps" section.
1.3.1.2	Reporting Engine (RE)	For more information, see "Configure Reporting Engine for Integration with Archer SecOps" section.
1.3.1.2	Respond	For more information, see "Configure Respond for Integration with Archer SecOps 1.3.1.2" section.
1.3.1.2	Archer Feeds	For more information, see "RSA Archer Feeds" section.

## Configure NetWitness to Work With Archer

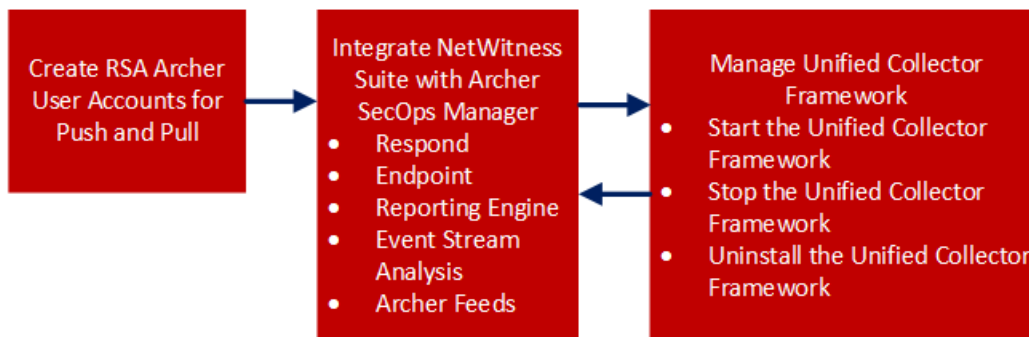
---

The RSA NetWitness SecOps Manager solution enables you to aggregate all actionable security alerts, allowing you to become more effective, proactive, and targeted in your incident response and SOC management. For more information on RSA NetWitness SecOps capabilities, see RSA Archer documentation on the [RSA Archer Community](#) or on the [RSA Archer Exchange Community](#).

The version of RSA Archer determines how NetWitness Suite will be integrated. See the *SecOps Installation Guide* for Archer platforms supported.

NetWitness SecOps Manager 1.3.1.2 integrates with NetWitness Suite using the RSA UCF (Unified Collector Framework) which comprises of Security Analytics Incident Management (IM) integration service and SecOps Watchdog service.

This figure represents the flow of NetWitness Suite 11.0 integration with NetWitness SecOps Manager 1.3.1.2.



### Create RSA Archer User Accounts for Push and Pull

You must create a user account for the web service client to transfer data to the RSA Archer GRC Platform.

You require two RSA Archer user accounts to avoid conflicts while sending and receiving data from RSA NetWitness Suite.

**To create a user account for push and pull, perform the following:**

1. On RSA Archer UI, click **Administration > Access Control > Users > Add New**.
2. In the **First Name** and **Last Name** fields, enter a name that indicates that the UCF uses this account to push data into RSA Archer GRC. For example, UCF User, Push.

**Note:** When configuring the Pull account, enter a name that indicates that the UCF uses this account to pull data from RSA Archer GRC. For example, UCF User, Pull.

3. (Optional) Enter a user name for the new user account.

**Note:** If you do not specify a user name, the RSA Archer GRC Platform creates the user name from the first and last name entered when you save the new user account.

4. In the **Contact Information** section, in the **Email** field, enter an email address to associate with the new user account
5. In the **Localization** section, change the time zone to (UTC) Coordinated Universal Time.

**Note:** The UCF uses UTC time to baseline all the time-related calculations.

6. In the **Account Maintenance** section, enter and confirm a new password for the new user account.

**Note:** Make a note of the user name and password for the new user account that you just created. You need to enter these credentials when you set up the UCF to communicate with the RSA Archer GRC Platform through the web service client.

7. Clear the Force Password Change On **Next Sign-In** option.
8. In the **Security Parameter** field, select the security parameter that you want to use for this user.

**Note:** If you assign a default security parameter with a password change interval of 90 days, you also must update the user account password stored in the SA IM integration service every 90 days. To avoid this, you can optionally create a new security parameter for the SA IM integration service user account and set the password change interval to the maximum value allowed by your corporate standards.

9. Click the **Groups** tab, and perform the following:
  - a. In the **Groups** section, click **Lookup**.
  - b. In the **Available Groups** window, expand Groups.
  - c. Scroll down and select SOC: Solution Administrator and EM: Read Only.
  - d. Click **OK**.
10. Click **Apply**, then click **Save**.
11. If the machine language and regional settings of your RSA Archer GRC system are set to anything other than English-US, perform the following:
  - a. Open the user account you just created, and in the **Localization** section, in the Locale field, select **English (United States)**, and click **Save**.
  - b. On the Windows system hosting your RSA Archer GRC Platform, open Internet Information Services (IIS) Manager.

- c. Expand your RSA Archer GRC site, click **.Net Globalization**, in both the **Culture** and **UI Culture** fields, select **English (United States)**, and click **Apply**.
  - d. Restart your RSA Archer GRC site.
12. Repeat steps 1 – 11 to create a second user account for the UCF to pull data from RSA Archer GRC.

## Integrate NetWitness Suite With Archer SecOps Manager

You have to configure the system integration settings to manage incident workflow in RSA NetWitness SecOps Manager.

For information on how to configure system integration settings to manage incident workflow in RSA Archer Security Operations, see the "Configure Integration Setting to Manage Incidents in RSA Archer Security Operations" topic in the *NetWitness Respond Guide*.

## RSA Unified Collector Framework (UCF)

RSA NetWitness Suite integrates with RSA Archer SecOps Manager 1.3.1.2 using the RSA Unified Collector Framework (UCF). The RSA Unified Collector Framework (UCF) integrates with all supported SIEM tools and the RSA NetWitness SecOps Manager solution. When integrating the RSA NetWitness Suite Respond, you can manage the incident workflow in the NetWitness Suite Respond and allow analysts the option to escalate remediation tasks and open data breaches for management and remediation in the RSA Archer Security Operations Management solution. And, the Unified Collector Framework transports remediation tasks (created as Findings), data breaches, or both.

### Note:

- You must configure the same option in both RSA NetWitness Suite and the Unified Collector Framework.
- Integration of the RSA NetWitness Respond module with Reporting Engine or Event Stream Analysis can result in duplicate events and incidents created in RSA Archer SecOps Manager.

UCF supports multiple SIEM tools connections at the same time, such as supporting NetWitness Suite Reporting Engine, HP ArcSight, and NetWitness Suite Respond. However, different instances of the same SIEM tool are not supported, such as two NetWitness Suite servers connected to the same UCF.

## Prerequisites

- Install `RSA_Archer_Security_Operations_Management` package on Archer. See RSA Archer documentation [RSA Archer Community](#) or on the Content Tab

at [https://community.emc.com/community/connect/grc\\_ecosystem/rsa\\_archer\\_exchange](https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange).

- Install NetWitness SecOps Manager.
- Ensure you have NetWitness Suite 11.0 as it is compatible with NetWitness SecOps Manager 1.3.1.2.
- Ensure that the Respond is configured in RSA NetWitness Suite.

The RSA Unified Collector Framework (UCF) allows you to integrate your RSA Archer Security Operations Manager system with the following:

- NetWitness Suite Respond
- NetWitness Suite Reporting Engine
- NetWitness Suite Event Stream Analysis
- Archer Feeds

## Configure Respond for Integration with Archer SecOps

To configure Respond for Archer SecOps, perform the following in NetWitness Suite:

### Step 1: Select the Mode for NetWitness Suite Respond

1. Select **ADMIN > Services > Respond > Explore**.
2. Navigate to Respond/Aggregation/export.
3. Enable `archer-secops-integration-enabled` field to **true**.
4. Restart Respond service.

### Step 2: Configure NetWitness Suite Respond to forward alerts to UCF

1. Navigate to `C:\Program Files\RSA\SA IM integration service\cert-tool\certs` in Secops middleware box.
2. Copy both `keystore.cert.pem` and `rootcastore.cert.pem` from `certs` folder( to import folder of NW-server)  

```
cp rootcastore.crt.pem /etc/pki/nw/trust/import
```

```
cp keystore.crt.pem /etc/pki/nw/trust/import
```

**Note:** Before you copy the files from UCF to NetWitness Admin server, examine the files to remove any blank lines and save them.

3. SSH to NW-server box



- a. Run the update-admin-node command  

```
orchestration-cli-client --update-admin-node
```
- b. Restart the RabbitMQ service  

```
service rabbitmq-server restart
```
- c. Create user archer and set permissions for the virtual host '/rsa/system'  

```
rabbitmqctl add_user archer archer
```




  

```
rabbitmqctl clear_password archer
```

```
rabbitmqctl set_permissions -p /rsa/system archer ".*" ".*" ".*"
```

### Step 3: Forward Alerts to the NetWitness Suite Respond

- **To forward NetWitness Suite Event Stream Analysis alerts to NetWitness Respond, perform the following:**
  - a. Select **ADMIN > Services > ESA** service.
  - b. Select an Event Stream Analysis service and click  > **View > Config**.
  - c. Click the **Advanced** tab.
  - d. Ensure that the **Forward Alerts on Message Bus** checkbox is selected by default. If not, select the **Forward Alerts on Message Bus** checkbox and click **Apply**.
- **To forward NetWitness Suite Reporting Engine alerts to NetWitness Respond, perform the following:**
  - a. Select **ADMIN > Services > Reporting Engine** service.
  - b. Click  > **View > Config** for the Reporting Engine service.
  - c. Click the **General** tab.
  - d. In the **System Configuration** section, select the **Forward Alerts to Respond** checkbox and click **Apply**.
- **To forward NetWitness Suite Malware Analysis alerts to NetWitness Respond, perform the following:**
  - a. Select **ADMIN > Services > Malware Analysis** service
  - b. Click  > **View > Config** for the Malware Analysis service.
  - c. Click the **Auditing** tab.
  - d. In the **Respond Alerting** section, verify that the **Enabled Config Value** checkbox is selected. If the checkbox is not selected, select the checkbox, and click **Apply**.

## Step 4: Forward Endpoint Alerts to the NetWitness Suite Respond

RSA Endpoint alerts can be sent to RSA Archer GRC through NetWitness Respond. For more information on how to Configure NetWitness Endpoint Alerts via Message Bus. See "Configure NetWitness Endpoint Alerts via Message Bus" topic in *NetWitness Endpoint Integration Guide*.

## Step 5: Aggregate Alerts into Incidents

Alerts coming into NetWitness Respond can be automatically aggregated into incidents and forwarded to RSA Archer Security Operations Management. Aggregation rules are automatically run every minute and aggregate the alerts into incidents based on the match conditions and grouping options selected. For more information on aggregating alerts, see the "Configure Alert Sources to Display Alerts in Respond" topic in the *NetWitness Respond Configuration Guide*.

### To configure alert aggregation:

1. Select **CONFIGURE > Incident Rules**.
2. To enable the rules provided out of the box, perform the following:
  - a. Double-click the rule.
  - b. Select **Enabled**.
  - c. Click **Save**.
  - d. Repeat steps a-c for each rule.
3. To add a new rule, do the following:
  - a. Click **+**.
  - b. Select **Enabled**.
  - c. Complete the following fields:
    - Rule Name
    - Action
    - Match Conditions
    - Grouping Options
    - Incident Options
    - Priority
    - Notifications
4. Click **Save**.

## Configure Endpoints in RSA Unified Collector Framework

Endpoints provide the connection details required for the UCF to reach both your RSA NetWitness Suite and RSA Archer GRC systems.

**Note:** Some endpoints are necessary to use different integrations. The following list shows the mandatory endpoints.

### Mandatory Endpoint Integration

- Archer Push endpoint
- Archer Pull endpoint
- Mode selection: SecOps or Non SecOps mode.

**Note:**

- If Non SecOps mode is selected, incidents are managed in NetWitness Suite Respond instead of RSA Archer Security Operations Management.
- You must configure the port depending on the protocol (TCP, UDP, or secure TCP).
- Ensure the certificate subject name for your RSA Archer GRC server matches the hostname.

### Procedure

1. On the UCF system, open the Connection Manager, as follows:
  - a. Open a command prompt.
  - b. Change directories to `<install_dir>\SA IM integration service\data-collector`.
  - c. Enter:  

```
runConnectionManager.bat
```
2. In the **Connection Manager**, enter **1** for Add Endpoint.
3. Add an endpoint for pushing data to RSA Archer Security Operations Management, as follows:
  - a. Enter the number for Archer.

**Note:** SSL must be enabled to add the RSA Archer endpoints.

- b. For the endpoint name, enter **push**.
- c. Enter the URL of your RSA Archer GRC system.
- d. Enter the instance name of your RSA Archer GRC system.

- e. Enter the user name of the user account you created to push data into your RSA Archer GRC system.
  - f. Enter the password for the user account you created to push data into your RSA Archer GRC system, and confirm the password.
  - g. When asked whether this account is used for pulling data, enter **False**.
4. Add an endpoint for pulling data from RSA Archer Security Operations Management, as follows:
- a. Enter the number for Archer.

**Note:** SSL must be enabled to add the RSA Archer endpoints.

- b. For the endpoint name, enter **pull**.
  - c. Enter the URL of your RSA Archer GRC system.
  - d. Enter the instance name of your RSA Archer GRC system.
  - e. Enter the user name of the user account you created to pull data from your RSA Archer GRC system.
  - f. Enter the password for the user account you created to pull data from your RSA Archer system, and confirm the password.
  - g. When asked whether this account is used for pulling data, enter **True**.
5. Add an endpoint for RSA NetWitness Suite
- For RESPOND
    - a. Enter the number for Security Analytics IM.
    - b. Enter a name for the endpoint.
    - c. Enter the SA Host IP address.
    - d. For SA Messaging Port, enter **5671**.
    - e. Enter the target queue for remediation tasks. Selecting All processes both the RSA Archer Integration (GRC) and IT Helpdesk (Operations).
    - f. To not automatically add certificates to the NetWitness Suite trust store, perform the following:  
Enter **No**.

- g. In UCF connection manager, select the mode, as follows:
    - i. Enter the number for Mode Selection.
    - ii. Select one of the following options:
      - Manage incident workflow in RSA NetWitness Suite.
      - Manage incident workflow exclusively in RSA Archer Security Operations Management.
  - For Reporting Engine and Event Stream Analysis
    - a. To use third-party integrations, add the Syslog Server Endpoint, as follows:
      - i. Enter the number for Syslog Server Endpoint.
      - ii. Enter the following:
        - User defined name
        - SSL Configured TCP port number

**Note:** Defaults to 1515. If you do not want to host the Syslog server in this mode, enter **0**.

      - TCP port number - Enter the TCP port if the Syslog client sends the Syslog message in TCP mode.

**Note:** Defaults to 1514. If you do not want to host the Syslog server in this mode, enter **0**.



      - UDP port number - Enter the UDP port if the Syslog client sends the Syslog message in UDP mode.

**Note:** Defaults to 514. If you do not want to host the Syslog server in this mode, enter **0**.

By default, the Syslog server will run in the above three modes, unless it is disabled by entering **0**.
    - b. To test the Syslog client, enter the number for Test Syslog Client. Use the Test Syslog client with the files from `<install_dir>\SA IM integration service\config\mapping\test-files\`.
6. In the Connection Manager, enter **5** to test each endpoint.

## Configure Reporting Engine for Integration with NetWitness SecOps Manager

To configure Syslog Output Action for the Reporting Engine, perform the following:

1. Select **ADMIN > Services**.
2. Select your Reporting Engine Service, and click   **View > Config**.
3. Click the **Output Actions** tab.
4. In the **NetWitness Suite Configuration** section, in the **Host Name** field, enter the host name or IP address of your Reporting Engine server.
5. In the **Syslog Configuration** section, add the Syslog Configuration as follows:
  - a. In the **Server Name** field, enter the hostname of the UCF.
  - b. In the **Server Port** field, enter the port that you selected in the UCF Syslog configuration.
  - c. In the **Protocol** field, select the transport protocol.

**Note:** If you select Secure TCP, SSL must be configured.

6. Click **Save**.



### To Configure NetWitness Suite Reporting Engine SSL for Secure Syslog Server:

If the Syslog server is configured with Secure TCP, configure the SSL.

1. Copy the certificate `keystore.crt.der` from the UCF machine to NetWitness Suite server box at `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.131-2.b11.e17_3.x86_64/jre/lib/security`
2. Run the following command:

```
keytool -import -file keystore.crt.der -alias ucf-syslog -keystore /etc/pki/nw/trust/truststore.jks -storepass changeit
```

**Note:** Do not copy and paste the above code. Type it in to avoid errors.

3. Enable **ServerCertificateValidationEnabled** to **true**:
  - Navigate to **ADMIN > Service**.
  - Click   **> View > Explore** of the Reporting Engine service .

- Expand **com.rsa.soc.re** > **Configuration** > **SSLContextConfiguration**.
  - Expand **sslContextConfiguration** and set **ServerCertificateValidationEnabled** to **true**.
4. Restart the Reporting Engine service.

#### To Configure Rules in NetWitness Suite:

1. Click **MONITOR > Reports > Manage**.  
The Manage tab is displayed.
2. In **Rule Groups** panel, click **+**.
3. Enter a name for the new group.
4. Select the group you created, and in the Rule toolbar, click **+**.
5. In the **Rule Type** field, select NetWitness DB.
6. Enter a name for the rule.
7. Enter values in the **Select** and **Where** fields based on the rule that you want to create.

**Note:** Add the Syslog configuration with the Syslog name set above.

8. Click **Save**.

**Note:** To see the same number of alerts in the Reporting Engine and RSA Archer GRC, ensure that you've selected Once for execute in both the Syslog and Record tabs.

#### To Add Alert Templates for the Reporting Engine in NetWitness Suite:

The UCF syslog configuration comes with out-of-the-box alert templates that you can use when you create an alert with a syslog output action. These templates define the criteria used to aggregate alerts into incidents in your RSA Archer GRC Platform.

The sample templates are located in the following location on the UCF system:

```
<install_dir>\SA IM integration service\config\mapping\templates\SecOps_  
SA_Templates
```

1. Click **MONITOR > Reports > Manage > Alerts**.
2. Click the **Template** tab.
3. Click **+**.

**Note:** After you copy the template in the Create/Modify Template window, make sure to replace `cs25=${sa.host}` `cs25Label=sahost` to `cs25=${nw.host}` `cs25Label=nwhost`.

1. In the **Name** field, enter a name for the alert template.
2. In the **Message** field, enter the alert message.
3. Click **Create**.
4. Repeat steps 3 to 6 for each alert template that you want to add.

### To Configure Alerts in NetWitness Suite:

In RSA NetWitness Suite Reporting Engine, an alert is a rule that you can schedule to run on a continuous basis and log its findings to several different alerting outputs.

1. Click **MONITOR > Reports > Manage > Alerts**.
2. Click **+**.
3. Select **Enable**.
4. Select the rule you created.
5. Select **Push to Decoders**.

**Note:** If you do not enter a value in this field, the link in the RSA Archer Security Alerts application to RSA NetWitness Suite will not work.

6. From the Data Sources list, select your data source.
7. In the **Notification** section, select **Syslog**.
8. Click **+**.
9. Complete the Syslog configuration fields.
10. In the **Body Template** field, select the template that you want to use for this Syslog alert.
11. Click **Save**.

## Configure Event Stream Analysis for Integration with Archer SecOps

### To Configure Event Stream Analysis Syslog Notification Settings in NetWitness Suite:

1. Click **ADMIN > System > Global Notifications**.
2. Click the **Output** tab.
3. Define and enable an Event Stream Analysis Syslog notification.
4. Click the **Servers** tab.
5. Define and enable a Syslog notification server.
6. In the Syslog Server Configuration section, enter the following:



### Field Description:

- Name - Specify the custom name
- Server IP (Hostname) - Specify the hostname or IP Address of the system on which you installed the UCF.
- Port - Specify the port number on which you want the UCF to listen for.
- Facility - Specify the Syslog facility
- Protocol - Select the protocol.

7. Click **Save**.

### To Configure NetWitness Suite Event Stream Analysis SSL for Secure Syslog Server:

If the Syslog server is configured with Secure TCP, configure the SSL.

1. Select **ADMIN > Services**.
2. Select the Event Stream Analysis service. Go to **Explore > Configuration > SSL**.
3. Set **ServerCertificateValidationEnabled** to **true**.
4. Copy the `rootcastore.cert.pem` from UCF machine to Event Stream Analysis server to `/etc/pki/ca-trust/source/anchors`.
5. Run the following command:  

```
update-ca-trust
```
6. Restart the Event Stream Analysis server.

### To Add Event Stream Analysis Alert Templates

The UCF syslog configuration comes with out-of-the-box alert templates that you can use when you create an alert with a syslog output action. These templates define the criteria used to aggregate alerts into incidents in your RSA Archer GRC Platform.

The sample templates are located in the following location on the UCF system:

```
<install_dir>\SA IM integration service\config\mapping\templates\SecOps_
SA_
Templates\SecOps_SA_ESA_templates.txt
```

1. Select **ADMIN > System > Global Notifications**.
2. Click the **Templates** tab.
3. Click **+**.
4. In the **Template Type** field, select Event Stream Analysis.
5. In the **Name** field, enter the name for the template.

6. (Optional) In the **Description** field, enter a brief description for the template.
7. In the **Template** field, enter the alert message.
8. Click **Save**.
9. Repeat steps 3 – 8 for each alert template that you want to add.

### **To Create Event Stream Analysis Rules**

1. Click **CONFIGURE > ESA Rules**.
2. In the **Rule Library**, click **+**.
3. Select **Rule Builder**.
4. In the **Rule Name** field, enter a name for the rule.
5. In the **Description** field, enter a description for the rule.
6. Select the **Severity**.
7. In the **Condition** section, do the following:
  - a. Click **+** to build a statement.
  - b. Enter a name, select a condition type, and add meta data/value pairs for your statement.
  - c. Click **Save**.
  - d. Repeat steps a – c until you have built all your statements for the rule.
8. In the **Notifications** section, select **Syslog**.
9. Select the notification, Syslog server, and template that were created previously.
10. Click **Save** and **Close**.
11. Click **Configure > Deployments**.
12. Click **+** for Event Stream Analysis services section.
13. Select the Event Stream Analysis Service.
14. Click **Deploy Now**.
15. In the **Event Stream Analysis Rules** section, click **+** to choose the Event Stream Analysis Rule that you created, and click **Deploy Now**.


## RSA Archer Feeds

By default, only the IP Address and Criticality Rating fields in the RSA Archer Devices application are fed into RSA NetWitness Suite by the SA IM Integration Service. You can customize the Enterprise Management plug-in to include the Business Unit and Facility fields that are cross-referenced in the Devices application in the feed. For more details, see Archer documentation at [https://community.emc.com/community/connect/grc\\_ecosystem/rsa\\_archer](https://community.emc.com/community/connect/grc_ecosystem/rsa_archer) or [https://community.emc.com/community/connect/grc\\_ecosystem/rsa\\_archer\\_exchange](https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange).

**Note:** If you plan to feed Business Unit and Facility information from your RSA Archer GRC Platform into Live, you must also add keys for these fields to the `index-concentrator-custom.xml` file.

## Update the Concentrator and Decoder Services

The SA IM Integration Service in NetWitness SecOps manager manages the files for a custom feed and deposits these files in a local folder that you specify when you configure the Enterprise Management Endpoint. The Live module of RSA NetWitness Suite retrieves the feed files from this folder. Live then pushes the feed to the Decoders, which start creating metadata based on captured network traffic and the feed definition. To make each Concentrator aware of the new metadata created by the Decoders, you must edit the `index-concentrator-custom.xml`, `index-logdecoder-custom.xml`, and `index-decoder-custom.xml` files.

1. Select **ADMIN > Services**.
2. Select your Concentrator, and select  > **View > Config**.
3. Click the **Files** tab.
4. From the drop-down list, select `index-concentrator-custom.xml`. Do one of the following:
  - If content already exists in the file, add a key for the new meta data element as follows:

```
<key description="Criticality" format="Text" level="IndexValues"
name="criticality" defaultAction="Open"/>
```

**Note:** Do not copy and paste code. Type it in to avoid errors.

- If the file is blank, add the following content:

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
<key description="Criticality" format="Text" level="IndexValues"
name="criticality" defaultAction="Open"/>
</language>
```

5. Click **Apply**.
6. To add multiple devices, do the following:

- a. Click **Push**.
  - b. Select the devices to which you want to push this file.
  - c. Click **OK**.
7. Repeat steps 1-7 for the Log Decoders and Index Decoders, using index-logdecoder-custom.xml and index-decoder-custom.xml.
  8. Restart the Concentrator and Decoder services.

## Add the RSA Archer Enterprise Management Endpoint in the UCF

1. In the UCF connection manager, select the mode, as follows:
  - a. Enter the number for Mode Selection.
  - b. Select one of the following options:
    - Manage incident workflow in RSA NetWitness Suite.
    - Manage incident workflow exclusively in RSA Archer Security Operations Management.
2. Add the RSA Archer Enterprise Management Endpoint, as follows:
  - a. Enter the number for Enterprise Management.
  - b. Complete the fields in the table below.

Field	Description
Endpoint Name	Optional endpoint name.
Web Server Port	Defaults to 9090. Can be configured to host the web server url. The URL with the port number should be provided as the URL in NetWitness Suite live feed: http://hostname:port/archer/sa/feed
Criticality	<p>Criticality of the assets to be pulled from RSA Archer GRC.</p> <p>If <b>false</b>, pull assets with any criticality.</p> <p>If <b>true</b>, pull assets with only high criticality.</p> <p>To configure this manually, edit the em.criticality property in the collector-config properties file to provide a comma-separated list of criticalities: LOW, MEDIUM, HIGH.</p>

Field	Description
Feed Directory	Directory where the assets CSV file from RSA Archer GRC are saved. <b>Note:</b> The directory path provided must exist.
Web Server Username	Username for authenticating to the EM web server. <b>Note:</b> This is provided while configuring the NetWitness Suitelive feed.
Web Server Password	Password for authenticating to the EM web server. <b>Note:</b> This is provided while configuring the NetWitness Suite live feed.
SSL Mode	Defaults to No. If <b>No</b> , the URL uses http mode: http://hostname:port/archer/sa/feed  If you have not updated the host file, see "Update the RSA NetWitness Suite Host File" section.  <b>Note:</b> NetWitness Suite currently does not support Archer recurring feeds in SSL mode.

## Update the RSA NetWitness Suite Host File

1. Edit the host file on the NetWitness Suite server at the following location: vi /etc/hosts
2. Enter the following for the UCF host IP address:  
`<ucf-host-ip> <ucf-host-name>`
3. Restart NetWitness Suite server by running the following command:  
`service jetty restart`
4. While configuring the NetWitness Suite live feed, enter the hostname for the URL instead of the IP address and the port number configured for Enterprise Management endpoint in the UCF:  
`http: //<ucf-host-name> : <EM_Port>/archer/sa/feed.`
5. Verify that the connection works.

## Create a Recurring Feed Task

In order for RSA NetWitness Suite to download feed files from the NetWitness Respond Integration Service and push the feeds to Decoders, you must create a recurring feed task and define the feed settings.

**Note:** For RSA Archer SecOps 1.2: In order for RSA NetWitness Suite to download feed files from your RCF machine and push the feeds to Decoders, you must create a recurring feed task and define the feed settings. The procedure is similar to RSA Archer SecOps 1.3, with a few exceptions. See documentation on the [RSA Archer Exchange Community](#) for details.

1. Select **CONFIGURE > Custom Feeds**.
2. In the Feeds view, Click **+**.
3. Select **Custom Feed**, and click **Next**.
4. Select **Recurring**.

5. Enter a name for the feed.

6. In the URL field, enter the following:

`http://ucf_hostname/archer/sa/feed`

where `http :ucf_hostname_or_ip:port` is the address of your NetWitness Respond Integration Service system. For example: `http://10.10.10.10:9090`.

**Note:** If the Respond is running in SSL mode, the hostname must be used in the URL.

7. Select **Authenticated**.
8. In the **User Name** and **Password** fields, enter the credentials of the user account you created for RSA NetWitness Suite to use to access files on the NetWitness Respond Integration Service system.
9. Define the recurrence interval for the feed.
10. In the **Date Range** section, define a start and end date for the feed, and click **Next**.
11. Select each Decoder to which you want to push this feed, and click **Next**.
12. In the **Type** field, ensure that IP is selected.
13. In the **Index Column** field, select 1.
14. In the second column, set the Key value to criticality, and click **Next**.
15. Review your feed configuration details, and click **Finish**.

## Manage Unified Collector Framework

---

This section provides additional tasks for configuring and managing the RSA Unified Collector Framework (UCF) for Archer SecOps 1.3.1.2 Integration.

### Start the RSA Unified Collector Framework

1. Click **Control Panel > Administrative Tools > Services**.
2. Select RSA Unified Collector Framework.
3. Click **Start**.

### Stop the RSA Unified Collector Framework

1. Click **Control Panel > Administrative Tools > Services**.
2. Stop the RSA SecOps WatchDog Service.

**Note:** If you do not stop the Watchdog service, the Watchdog service starts the NetWitness Respond Service before intended.

3. Select RSA Unified Collector Framework.
4. Click **Stop**.

**Note:** If the service takes too long to shutdown, use the Task Manager to end the RSASAIMDCService.

### Uninstall the RSA Unified Collector Framework

1. Click **Control Panel > Programs and Features**.
2. Select **RSA Unified Collector Framework**.
3. Click **Uninstall**.

## Troubleshoot RSA Archer Integration

---

This section provides resolutions to common problems that you may encounter while configuring Archer SecOps 1.3.1.2 with NetWitness Suite Respond.

### Setting the CA Truststore

**Problem:** After adding the endpoint for NetWitness Suite Respond, the CA truststore fails to set.

**Resolution:**

1. Ensure that the SSH credentials for the NetWitness Suite host are valid.
2. If the credentials are correct, but the error still occurs, manually copy certificates.

### Remediation Tasks in RSA Archer Security Operations Manager

**Problem:** Remediation Tasks being pushed to the operations queue through the UCF are not appearing in RSA Archer Security Operations Management as Findings.

**Resolution:**

1. Open the Connection Manager:
  - Open a command prompt
  - Change directories to `<install_dir>\SA IM integration service\data-collector.`
  - Type: `runConnectionManager.bat`
2. Enter 2 to edit endpoint.
3. Enter 3 to NetWitness Suite Respond.
4. Ensure the Target Queue is set to All or Operations.

### Errors between RSA NetWitness Suite and RSA Unified Collector

#### Framework

**Problem:** In the `<install_dir>\SA IM integration service\logs\collector.log`, there are SSL errors between RSA NetWitness Suite and RSA Unified Collector Framework.

**Resolution:**



1. Verify that the SSL certificates are valid.

**Note:** NetWitness Suite Respond certificates are valid for two years.

2. If your certificates are expired, regenerate and copy the expired certificates.

**To regenerate and copy the certificates, do the following:**

1. In Command Prompt, go to `<install_dir>\SA IM integration service\data-collector`.
2. Enter: `runConnectionManager.bat`
3. Enter the number for Regenerate SA IM Integration Service Certificate.
4. In the NetWitness Suite Respond endpoint, in Connection Manager, enter the number for Edit Endpoint.
5. Enter Yes to copy the certificates automatically to the NetWitness Suite trust store.

**Note:** If certificates fail to copy, manually copy the certificates.

