NetWitness® Platform XDR

Version 12.1.0.0

Archer Integration Guide

NETWITNESS
Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

October, 2022

Contents

Archer Integration

Administrators can integrate NetWitness with Archer Cyber Incident & Breach Response to send alerts and incidents from NetWitness 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 10.6.5 to NetWitness 11.x, the Archer Cyber Incident & Breach Response integration is no valid, and must be re-configured.

The following table list the NetWitness 11.x integration options with Archer Cyber Incident & Breach Response Version 1.3.1.2.

Archer Cyber Incident & Breach Response Version	NetWitness 11.x Integration	Reference
1.3.1.2	ESA Correlation	See "Configure ESA Correlation for Integration with Archer Cyber Incident & Breach Response" section.
1.3.1.2	Reporting Engine (RE)	See "Configure Reporting Engine for Integration with Archer Cyber Incident & Breach Response" section.
1.3.1.2	Respond	See "Configure Respond for Integration with Archer Cyber Incident & Breach Response 1.3.1.2" section.
1.3.1.2	Archer Feeds	See "Archer Feeds" section.

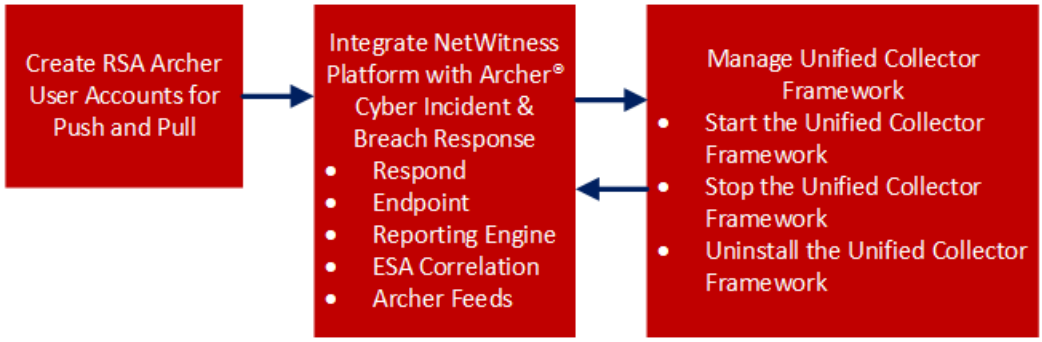
Configure NetWitness to Work With Archer

The Archer Cyber Incident & Breach Response 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 Archer Cyber Incident & Breach Response capabilities, see Archer documentation on the Archer Community or on the Archer Exchange Community.

This version of Archer determines how NetWitness will be integrated. For supported Archer platforms, see the *SecOps Installation Guide*.

Archer Cyber Incident & Breach Response1.3.1.2 integrates with NetWitness using the UCF (Unified Collector Framework), which comprises of NetWitness Respond integration service and Archer Cyber Incident & Breach Response Watchdog service.

This figure represents the flow of NetWitness 11.x integration with Archer Cyber Incident & Breach Response 1.3.1.2.



Create Archer User Accounts for Push and Pull

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

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

To create a user account for push and pull:

1. On the 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 Unified Collector Framework (UCF) uses this account to push data into 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 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 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** panel, 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 created. You need to enter these credentials when you set up the UCF to communicate with the 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** panel, 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** and click **Save**.
11. If the machine language and regional settings of your 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 Archer GRC Platform, open **Internet Information Services (IIS) Manager**.
    c. Expand your Archer GRC site, click **.Net Globalization**, in both the **Culture** and **UI Culture** fields, select **English (United States)**, and click **Apply**.
    d. Restart your Archer GRC site.
12. Repeat steps 1 – 11 to create a second user account for the UCF to pull data from Archer GRC.

Integrate NetWitness Platform With Archer Cyber Incident & Breach Response

You have to configure the system integration settings to manage incident workflow in Archer Cyber Incident & Breach Response.

For information on how to configure system integration settings, see the "Manage Incidents in Archer Cyber Incident & Breach Response" in the *NetWitness Respond Configuration Guide*.

Unified Collector Framework

NetWitness integrates with Archer Cyber Incident & Breach Response 1.3.1.2 using the UCF. The UCF integrates with all supported SIEM tools and the Archer Cyber Incident & Breach Response solution. After you configure the system integration settings, all incidents are managed in Archer Cyber Incident & Breach Response instead of NetWitness Respond. Incidents created before the integration will not be managed in Archer Cyber Incident & Breach Response.

Note:
• You must configure the same option in both NetWitness and the Unified Collector Framework.
• Integration of the NetWitness Respond module with Reporting Engine or ESA Correlation can result in duplicate events, alerts, and incidents created in Archer Cyber Incident & Breach Response.

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

Prerequisites

- Install the Archer Cyber Incident & Breach Response package on Archer. See Archer documentation Archer Community or on the Content Tab at https://www.archerirm.community/t5/exchange-overviews/archer-exchange-offering-list/ta-p/672315.
- Install Archer Cyber Incident & Breach Response 1.3.1.2.
- Ensure you have NetWitness 11.1 as it is compatible with Archer Cyber Incident & Breach Response 1.3.1.2.
- Ensure that Respond is configured inNetWitness.

The UCF allows you to integrate your Archer Cyber Incident & Breach Response system with the following:

- NetWitness Respond
- NetWitness Reporting Engine
- NetWitness ESA Correlation.
- Archer Feeds

Configure Respond for Integration with Archer Cyber Incident & Breach Response

Step 1: Select the Mode for NetWitness Respond

1. Go to  **(Admin) > Services**, select the **Respond Server** service, and select  > **View** > **Explore**.

2. Navigate to `respond/integration/export`.
3. Set the `archer-sec-ops-integration-enabled` field to **true**.
4. Restart the Respond service by running the following command:
   `systemctl restart rsa-nw-respond-server`

Step 2: Configure NetWitness Respond to Forward Alerts to UCF

1. Navigate to `C:\Program Files\RSA\SA IM integration service\cert-tool\certs` in the SecOps Middleware box.
2. Copy both `keystore.crt.pem` and `rootcastore.crt.pem` from the certs folder (to the import folder of NetWitess 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:
      `systemctl restart rabbitmq-server`
   c. Restart the SMS service:
      `systemctl restart rsa-sms.service`

      Note: This step is mandatory to avoid receiving the "message bus down" error message which indicates that the EventSourceMessagePublisher has failed to reconnect to RabbitMQ on restart. This can cause some features such as deleting event sources to function improperly.

   d. 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 Respond

- To forward NetWitness ESA Correlation alerts to the NetWitness Respond:
  a. Go to  **(Admin) > Services > ESA** service.
  b. Select an **ESA Correlation** service and select  **> View > Explore**.
  c. Navigate to the Correlation option in the left panel and select the Alert option.
  d. Edit the respond-enabled option to TRUE.
  e. Restart the Correlation server.

- To forward NetWitness Reporting Engine alerts to NetWitness Respond:
  a. Go to **(Admin) > Services > Reporting Engine** service.
  b. Select the **Reporting Engine** service, and then select **> View > Config**.
  c. Click the **General** tab.
  d. In the **System Configuration section**, select the **Forward Alerts to Respond** checkbox and click **Apply**.
- To forward NetWitness Malware Analysis alerts to NetWitness Respond:
  a. Go to **(Admin) > Services > Malware Analysis** service
  b. Select the **Malware Analysis** service, and select > **View** > **Config**.
  c. Click the **Auditing** tab.
  d. In the **Respond Alerting** panel, 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 Respond

You can forward Endpoint alerts to the 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" in the *NetWitness Endpoint Integration Guide*.

Step 5: Aggregate Alerts into Incidents

The Respond Server service consumes alerts from the message bus and normalizes the data to a common format (while retaining the original data) to enable simpler rule processing. It periodically runs rules to aggregate multiple alerts into an incident and set some attributes of the Incident (for example, severity, category, and so on). For more information on aggregating alerts, see the "Configure Alert Sources to Display Alerts in Respond View" topic in the *NetWitness Respond Configuration Guide*.

To configure alert aggregation:

1. Go to **(Configure) > Incident Rules**.
2. To enable the rules provided out-of- the-box:
   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:
   a. Click **Create Rule**.
   b. Select **Enabled**.
   c. Enter the values in the following fields:

- Rule Name
- Action
- Match Conditions
- Grouping Options
- Incident Options
- Priority
- Notifications

4. Click **Save**.

Configure Endpoints in Unified Collector Framework

Endpoints provide the connection details required for the UCF to reach both your NetWitness and 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 Respond instead of Archer Cyber Incident & Breach Response.
• You must configure the port depending on the protocol (TCP, UDP, or secure TCP).
• Make sure the certificate subject name for your 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 Archer Cyber Incident & Breach Response, as follows:
   a. Enter the number for Archer.

      Note: Enable SSL to add the Archer endpoints.

   b. For the endpoint name, enter **push**.

c. Enter the URL of your Archer GRC system.

d. Enter the instance name of your Archer GRC system.

e. Enter the user name of the user account you created to push data into your Archer GRC system.

f. Enter the password for the user account you created to push data into your Archer GRC system, and confirm the password.

g. When prompted if this account is used for pulling data, enter **False**.

4. Add an endpoint for pulling data from Archer Cyber Incident & Breach Response, as follows:

a. Enter the number for Archer.

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

b. For the endpoint name, enter **pull**.

c. Enter the URL of your Archer GRC system.

d. Enter the instance name of your Archer GRC system.

e. Enter the user name of the user account you created to pull data from your Archer GRC system.

f. Enter the password for the user account you created to pull data from your Archer system, and confirm the password.

g. When prompted if this account is used for pulling data, enter **True**.

5. Add an endpoint for NetWitness:

- For Respond

a. Enter the number for NetWitness 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 Archer Integration (GRC) and IT Helpdesk (Operations).

f. When prompted to automatically add certificates to the SA trust store, enter **No**.
The certificates are added manually in previous steps.

g. In UCF connection manager, select the mode, as follows:

i. Enter the number for Mode Selection.

ii. Select Manage incident workflow exclusively in Archer Cyber Incident & Breach Response from the drop-down.

> **Note:** Make sure you select the second option as the first option is not supported in NetWitness Platform 11.x release.

- For Reporting Engine and ESA Correlation
  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 runs 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 Archer Cyber Incident & Breach Response

To configure Syslog Output Action for the Reporting Engine:

1. Go to  **(Admin) > Services**.
2. Select the **Reporting Engine** service, and click  **View** > **Config**.
3. Click the **Output Actions** tab.
4. In the **NetWitness Platform Configuration** panel, in the **Host Name** field, enter the host name or IP address of the Reporting Engine server.
5. In the **Syslog Configuration** section, add the Syslog Configuration as follows:

a. In the **Server Name** field, enter the host name 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:** Configure SSL if you select Secure TCP.

6. Click **Save**.

To configure NetWitness Reporting Engine SSL for Secure Syslog Server:

1. Copy the certificate `keystore.crt.der` from the UCF machine to NetWitness server box at `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4.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 command. Type the command to avoid errors.

3. Enable **ServerCertificateValidationEnabled** to **true:**
   - Go to  **(Admin) > Services**.
   - Select  **> 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 by running the following command:
   `service rsasoc_re restart`

To configure rules in NetWitness Platform:

1. Go to **Reports > Manage**.
   The Manage tab is displayed.
2. In the **Rules > Groups** panel, click **+**.
3. Enter a name for the new group.
4. Select the group you created, and in the Rule toolbar, click **+**.
   1. In the **Rule Type** field, select **NetWitness Platform DB**.
5. Enter a name for the rule.
6. 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.

7. Click **Save**.

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

To add Alert Templates for the Reporting Engine in NetWitness Platform:

The UCF syslog configuration contains out-of-the-box alert templates that you can use to create an alert with a syslog output action. These templates define the criteria used to aggregate alerts into incidents in your 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. Go to **Reports > Manage > Alerts**.
2. Select the **Template** tab and 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`.

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

To Configure Alerts in NetWitness Platform:

In NetWitness 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. Go to **Reports > Manage > Alerts**.
2. Click +, select **Enable**, then Select the rule you created.
3. Select **Push to Decoders**.

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

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

Configure ESA Correlation for Integration with Archer Cyber Incident & Breach Response

To configure ESA Correlation Syslog Notification Settings in NetWitness:

1. Go to  **(Admin) > System > Global Notifications**.
2. Click the **Output** tab.
3. Define and enable an ESA Correlation 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.
   - Facility - Specify the Syslog facility.
   - Protocol - Select the protocol.
7. Click **Save**.

To configure NetWitness Platform ESA Correlation SSL for Secure Syslog Server:

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

1. Copy the `keystore.cert.pem` from UCF machine to NetWitness server.
2. Run the following command:

   ```
   security-cli-client --add-trusts --service integration-server --superuser-id admin --superuser-pwd netwitness --chain-file <path to keystore.cert.pem file>
   ```
3. Restart the integration server by running the following command:

   ```
   service rsa-nw-integration-server restart
   ```

To Add ESA Correlation Alert Templates

The UCF syslog configuration contains out-of-the-box alert templates that you can use to create an alert with a syslog output action. These templates define the criteria used to aggregate alerts into incidents in your 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 and click .
3. In the **Template Type** field, select ESA Correlation.
4. In the **Name** field, enter the name for the template.
5. 6. (Optional) In the **Description** field, enter a brief description for the template.

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

To Create ESA Correlation 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** panel:
   a. Click ✚ to build a statement.
   b. Enter a name, select a condition type, and add meta data/value pairs for the statement.
   c. Click **Save**.
   d. Repeat steps a – c until you have built all the 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 click **Close**.
11. In the Deployments section, click  .
12. Click ✚ and enter a deployment name.
13. Click ✚ for ESA Correlation services section.
14. Select the ESA Correlation Service.
15. In the Data Source section, click ✚ and select a data source.
16. Click **Save**.
17. In the **ESA Correlation Rules** section, click ✚ to select the ESA Correlation Rule that you created.
18. Click **Save**.
19. Click **Deploy Now**.

Archer Feeds

By default, only the IP address and Criticality Rating fields in the Archer Devices application are fed into NetWitness 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://www.archerirm.community/t5/exchange-overviews/archer-exchange-offering-list/ta-p/672315.

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

Update the Concentrator and Decoder Services

The SA IM Integration Service in Archer Cyber Incident & Breach Response 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 NetWitness retrieves the feed files from this folder. Live then pushes the feed to the Decoders, which start creating metadata based on the captured network traffic and the feed definition. To enable the Concentrator to detect a new metadata created by the Decoders, make sure to edit the `index-concentrator-custom.xml`, `index-logdecoder-custom.xml`, and `index-decoder-custom.xml` files.

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

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

     Note: Do not copy and paste above command . Type the command 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:
   a. Click **Push**.
   b. Select the devices to which you want to push this file.
   c. Click **OK**.

7. Repeat steps 1 to 6 for the Log Decoders and Index Decoders, using index-logdecoder-custom.xml and index-decoder-custom.xml.
8. Restart the Concentrator and Decoder services by running the following commands:
```
service nwdecoder restart
service nwconcentrator restart
```

Add the Archer Enterprise Management Endpoint in UCF

1. In the UCF connection manager, select the mode:
   a. Enter the number for Mode Selection.
   b. Select one of the following options:
      - Manage incident workflow in NetWitness.
      - Manage incident workflow exclusively in Archer Cyber Incident & Breach Response.
2. Add the Archer Enterprise Management Endpoint:
   a. Enter the number for Enterprise Management.
   b. Enter the values in the fields as described in the table below.

Field	Description
Endpoint Name	Optional endpoint name.
Web Server Port	Defaults to 9090. You can configure this to host the web server url by providing the URL with the port number as in the NetWitness live feed: http://hostname:port/archer/sa/feed.
Criticality	Criticality of the assets to be pulled from Archer GRC. If **false**, pull assets with any criticality. If **true**, pull assets with only high criticality. 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.
Feed Directory	Directory where the assets CSV file from Archer GRC are saved. **Note:** The directory path provided must exist.
Web Server Username	Username for authenticating to the EM web server.
Web Server Password	Password for authenticating to the EM web server.

Field	Description
SSL Mode	Defaults to No. If **No**, the URL uses `http mode: http://hostname:port/archer/sa/feed` If you have not updated the host file, see "Update the NetWitness Host File" section. **Note:** NetWitness currently does not support Archer recurring feeds in SSL mode.

Update the NetWitness Platform Host File

1. Edit the host file on the NetWitness 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 server by running the following command:

   `service jetty restart`
4. While configuring the NetWitness live feed, enter the host name 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

For NetWitness 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 Archer Cyber Incident & Breach Response 1.2: For NetWitness to download feed files from the UCF machine and push the feeds to Decoders, you must create a recurring feed task and define the feed settings. The procedure is similar to Archer Cyber Incident & Breach Response 1.3, with a few exceptions. See documentation on the 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 the NetWitness Respond Integration Service system. For example: `http://<ucf-host-name>` .
7. Select **Authenticated**.

8. In the **User Name** and **Password** fields, enter the credentials of the user account you created in the Add the Archer Enterprise Management Endpoint in UCF procedure.
9. Define the recurrence interval for the feed.
10. In the **Date Range** panel, 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, amke sure 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 UCF for Archer Cyber Incident & Breach Response 11.3.1.2 Integration.

Start the Unified Collector Framework

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

Stop the Unified Collector Framework

1. Click **Control Panel > Administrative Tools > Services**.
2. Stop the Archer Cyber Incident & Breach Response WatchDog Service.

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

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 Unified Collector Framework

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

Troubleshoot Archer Integration

This section provides resolutions to common problems that you may encounter while configuring Archer Cyber Incident & Breach Response 1.3.1.2 with NetWitness Respond.

Problem	Solutions
After adding the endpoint for NetWitness Respond, the Certificate Authority truststore fails to set. **Resolution**	1. Make sure that the SSH credentials for the NetWitness host are valid. 2. If the credentials are correct, but the error still occurs, manually copy certificates.
Remediation Tasks being pushed to the operations queue through the UCF are not appearing in Archer Cyber Incident & Breach Response as Findings.	1. Open the Connection Manager using the command prompt: • `Change directories to <install_dir>\SA IM integration service\data-collector.` • `Type: runConnectionManager.bat` 1. Enter **2** to edit endpoint. 2. Enter **3** to NetWitness Respond. 3. Make sure the Target Queue is set to **All** or **Operations**.
In the `<install_dir>\SA IM integration service\logs\collector.log`, there are SSL errors between NetWitness and RSA Unified Collector Framework.	1. Verify that the SSL certificates are valid. **Note:** NetWitness 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:** 1. In the Command Prompt, go to `<install_dir>\SA IM integration service\data-collector.` 2. Enter `runConnectionManager.bat` 3. Enter the number for Regenerate NetWitness RespondIntegration Service Certificate.

Problem	Solutions
NetWitness unable to forward incidents to UCF.	4. In the NetWitness Respond endpoint, in Connection Manager, enter the number for Edit Endpoint. 5. Enter **Yes** to copy the certificates automatically to the NetWitness trust store. **Note:** If certificates fail to copy, manually copy the certificates. 1. In the collector config (C:\PROGRAM FILES\RSA\SA IM INTEGRATION SERVICE\CONFIG\collector-config), change the following: im.virtualhost=/rsa/im/integration to im.virtualhost=/rsa/system 2. Restart UCF. For more information on restarting UCF, see Start the Unified Collector Framework. 3. In the data collector (C:\PROGRAM FILES\RSA\SA IM INTEGRATION SERVICE\data-collector), double click on the following file to run it. runConnectionmanager.bat