

NetWitness[®] Platform

Version 12.4.1.0

UEBA Configuration Guide

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

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and 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 RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

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 NetWitness Community. 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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA 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." RSA 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.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at <https://www.netwitness.com/standard-form-agreements/>.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

June, 2024

Contents

Introduction	5
UEBA Supported Sources by Schema	5
Authentication Schema	5
File Schema	5
Active Directory Schema	6
Endpoint Process Schema	6
Endpoint Registry Schema	6
Packet Schema	6
Configure Custom Feeds and Application Rules for VPN Vendors	6
Configure Custom Feeds for Supporting VPN Vendors	6
Configure Application Rules for Supporting VPN Vendors	11
How to verify if UEBA is consuming the Custom VPN types	12
UEBA Configuration	15
Configure Multiple UEBA Servers	15
Best Practices to Add and Remove Schemas for Multiple UEBA Servers	16
ueba-server-config script	16
reset-presidio script	17
Add a Schema without Rerunning the UEBA	18
UEBA Indicator Forwarder	19
Update Data Source Details	19
Add Features for UEBA Packet Schema	19
Add the Hunting Pack:	19
Assign User Access to UEBA	20
Create an Analysts Role	21
Enable User Entity Behavior Analytics Incident Rule	22
Enable or Disable Modeled Behaviors for Users	23
Removal of Packetbeat Service	24
Learning Period Per Scale	25
Learning Period Per Scale for 12.4	25
Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)	25
Virtual Machine	26
Learning Period Per Scale for 12.4 Multiple UEBA Servers	30
Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)	30
Learning Period Per Scale for 12.3.1	33
Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)	33
Virtual Machine	35
Learning Period Per Scale for 12.3.1 Multiple UEBA Servers	37

Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)	37
Learning Period Per Scale for 12.3	40
Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)	40
Virtual Machine	41
Learning Period Per Scale for 12.3 Multiple UEBA Servers	43
Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)	43
Learning Period Per Scale (from 11.5.1 version to 12.2.0.1)	45
Physical Machine	45
Virtual Machine	46
Learning Period Per Scale for 11.5	48
Physical Machine	48
Virtual Machine	50
Troubleshooting UEBA Configurations	53
Task Failure Issues in Airflow	53
MongoDB I/O Operations Slowness Issue	55
User Interface Inaccessible	56
Get UEBA Configuration Parameters	56
Check UEBA Progress Status using Airflow	57
Check if data is received on the UEBA by Kibana	58
Scaling Limitation Issue	59
UEBA Policy Issue	60
Troubleshoot Using Kibana	60
Troubleshoot Using Airflow	61

Introduction

NetWitness® UEBA configuration is designed for analysts to perform analytics for leveraged data collected from netwitness logs and networks to perform UEBA analytics.

Note: Mixed mode is not supported for UEBA in NetWitness Platform. The NetWitness server, and UEBA must all be installed and configured on the same NetWitness Platform version.

UEBA Supported Sources by Schema

Note: Please deploy the latest parsers from NetWitness Live to enable support for all the models and VPN devices.

Authentication Schema

- Windows Logon and Authentication Activity - Supported Event IDs: 4624, 4625, 4769, 4648 (device.type=winevent_snare|winevent_nic)
- RSA SecurID Token - device.type = 'rsaacesrv' ec.activity = 'Logon'
- RedHat Linux - device.type = 'rhlinux'
- Windows Remote Management - Supported Event IDs: 4624,4625,4769,4648 (device.type=windows)
- VPN Logs - event.type = 'vpn' ec.activity = 'logon'

Note: NetWitness has tested and verified the functionality of Juniper, Citrix NetScaler, Palo Alto Networks, Cisco Adaptive Security Appliance (ASA) and Fortinet VPNs under the Authentication schema of UEBA. For any VPN to be considered under the Authentication module, the following metadata must be present in the respective VPN vendor's logs:
(event.type = 'vpn' && country.src exists && user.dst exists && ec.activity = 'logon')

- Azure AD Logs - device.type = 'microsoft_azure_signin_events'

Note: Make sure you have configured the Azure Monitor plugin in your deployment. This enables UEBA to run a query for Azure AD log events for monitoring purposes in the correct format. For more information on how to configure the Azure Monitor plugin, see the *Azure Monitor Event Source Configuration Guide*.

File Schema

- Windows File Servers - Supported Event IDs: 4663,4660,4670,5145 (device.type=winevent_snare|winevent_nic)
- device.type=windows

Active Directory Schema

- Windows Active Directory - Supported Event IDs:
4741,4742,4733,4734,4740,4794,5376,5377,5136,4764,4743,4739,4727,4728,4754,4756,4757,4758,4720,4722,4723,4724,4725,4726,4738,4767,4717,4729,4730,4731,4732 (device.type=winevent_snare|winevent_nic)
- device.type=windows

Endpoint Process Schema

- Endpoint Process - Category = 'Process Event'

Endpoint Registry Schema

- Endpoint Registry - Category = 'Registry Event'

Packet Schema

- TLS - Service 443 (direction='outbound')

Note: The TLS Packet requires adding the hunting package as described in [Add required features for UEBA Packets Schema](#).

Configure Custom Feeds and Application Rules for VPN

Vendors

Note: The approaches described below can be used temporarily until official support for this VPN vendor is added to NetWitness UEBA. To request official support for the required VPN vendor, please contact your [NetWitness Customer Support](#) team.

There are two methods to add support for VPN Vendors:


- [Configure Custom Feeds for Supporting VPN Vendors](#)
- [Configure Application Rules for Supporting VPN Vendors](#)

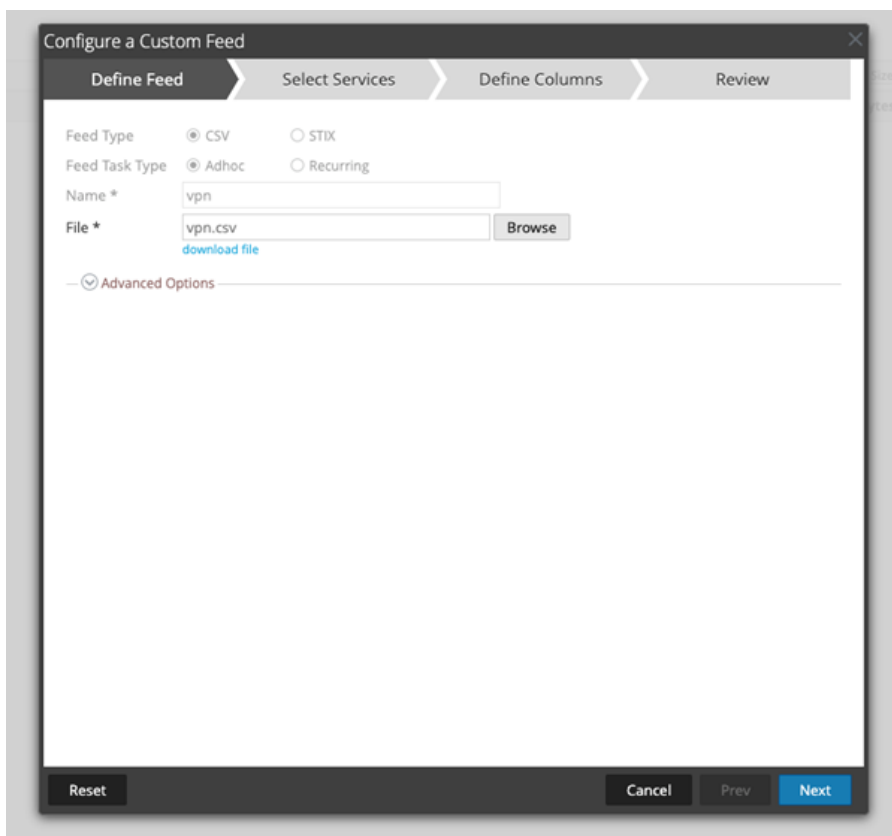
Configure Custom Feeds for Supporting VPN Vendors

To include VPN vendors that UEBA does not support out-of-the-box, you can create custom feeds and include those VPN vendors as part of UEBA processing. Before writing the custom feed, the user must first distinguish between success and failure events related to their VPN vendor. The following is a list of meta keys that UEBA considers when analyzing a VPN event. To receive support for any VPN vendor on UEBA, it is mandatory for these meta keys to be present:

1. event.time
2. user.dst
3. device.type
4. country.src
5. city.src
6. event.type = vpn
7. ec.outcome = success or failure
8. ec.activity = logon

The following is an example of deploying a custom feed for Palo Alto Networks CEF logs.

1. Go to  (Configure) > **Custom Feeds** and select **Custom Feed** and upload a .csv file containing CEF logs and click **Next**.



For example, Palo Alto Networks has a meta result = success for success events, and an event.desc = globalprotect, which can be used as callbacks to append additional meta keys such as event.type, ec.outcome, and ec.activity to logs.

2. Select the Decoders and Log Decoders and click **Next**.

3. Select the callback keys to `result` and `event.desc` from the drop-down and add the additional meta keys such as `event.type`, `ec.outcome`, and `ec.activity` to logs and click **Next**.

Configure a Custom Feed

Define Feed | Select Services | **Define Columns** | Review

Define Index

Type: IP IP Range Non IP

Index Column(S): 1 Service Type: 0 Truncate Domain Ignore Case

Callback Key (S): result event.desc

Define Values

Column	1 (index)	2	3	4
Key		ec.outcome	event.type	ec.activity
	success	success	vpn	logon

Reset Cancel Prev **Next**

4. Review the details and click **Finish**.

Configure a Custom Feed

Define Feed | Select Services | Define Columns | **Review**

Feed Details

Name: vpn
CSV File: vpn.csv

Service Details

Services: endpointloghybrid - Log Decoder, esaprimary - Contexthub Server

Column Mapping Details

Index Type: Other
Callback Key(s): result, event.desc
Truncate Domain: false
Ignore Case: true
Service Type: 0

Value Columns

1 Index | 2 ec.outcome | 3 event.type | 4 ec.activity

Reset | Cancel | Prev | **Finish**

Similarly, you need to deploy one more custom feed for failure event. For detailed procedure on creating the custom feed, see the topic [Creating a Custom Feed](#) in the *Live Services Management Guide*.

Note: Two custom feeds must be created and deployed, one for successful and another for failed events.

- Ensure the `ec.outcome` value is set to **success** for all successful logon events.
- Ensure the `ec.outcome` value is set to **failure** for all failure logon events.

IMPORTANT: To ensure that UEBA always consider logon events for analytics, all of these events must contain the 8 meta keys listed above.

The following is an example of how it is demonstrated for CEF events of Palo Alto Networks. Before using custom feeds, these are the list of meta keys available on the **Investigate > Events** page.

SESSIONID 267030	PROCESS logforwarder	LATDEC.SRC 42.6481
TIME 08/16/2023 04:10:56 pm	VERSION 2.0	LONGDEC.SRC -71.3343
SIZE 1.35 KB	EVENT.TYPE GLOBALPROTECT	ISP.SRC Comcast Cable
DID endpointloghybrid	EVENT.DESC globalprotect	ORG.SRC Comcast Cable
MEDIUM 32	USER.DST [REDACTED]	RESULT success
DEVICE.TYPE palo_alto_networks_if	HOST.SRC *****	ALIAS.HOST GPGW_294546_us-east-1_*****
HEADER.ID 0011	IP.SRC [REDACTED]	DEVICE.DISC 100
MSG.ID palo_alto_networks_if	NETNAME other src	DEVICE.DISC.TYPE palo_alto_networks_if
ALIAS.HOST logfwd20-6162ff2a-2ed0-****-*****- taskmanager-9df7m	COUNTRY.SRC United States	SOURCEFILE gateway-auth.log
	CITY.SRC Lowell	

The following is the list of meta keys seen on the **Investigate > Events** page after deploying a custom feed.

SESSIONID 267031	PROCESS logforwarder	CITY.SRC Lowell
TIME 08/16/2023 04:15:06 pm	VERSION 2.0	LATDEC.SRC 42.6481
SIZE 1.35 KB	EVENT.TYPE GLOBALPROTECT	LONGDEC.SRC -71.3343
DID endpointloghybrid	EVENT.DESC globalprotect	ISP.SRC Comcast Cable
MEDIUM 32	USER.DST [REDACTED]	ORG.SRC Comcast Cable
DEVICE.TYPE palo_alto_networks_if	HOST.SRC *****	RESULT success
HEADER.ID 0011	IP.SRC [REDACTED]	EC.OUTCOME success
MSG.ID palo_alto_networks_if	NETNAME other src	EVENT.TYPE vpn
ALIAS.HOST logfwd20-6162ff2a-2ed0-****-*****- taskmanager-9df7m	COUNTRY.SRC United States	EC.ACTIVITY logon

ALIAS.HOST GPGW_294546_us-east-1_*****
DEVICE.DISC 100
DEVICE.DISC.TYPE palo_alto_networks_if
SOURCEFILE gateway-auth.log

Note: It is recommended that users parse the raw logs of VPN vendors from NetWitness.

IMPORTANT: The custom feed must be deployed on all Decoders that contain VPN Data.

Note: NetWitness recommends you to use multiple metas for callback keys and the right callback meta keys based on the available meta keys for success and failure events when deploying feeds.

Configure Application Rules for Supporting VPN Vendors

Before deploying the application rules, the user must first distinguish between success and failure events related to their VPN vendor. The following is a list of meta keys that UEBA considers when analyzing a VPN event. To receive support for any VPN vendor on UEBA, it is mandatory for these meta keys to be present:

1. `event.time`
2. `user.dst`
3. `device.type`
4. `country.src`
5. `city.src`
6. `event.type = vpn`
7. `ec.outcome = success or failure`
8. `ec.activity = logon`

This example describes how to use application rules to support VPN vendors.

In this case, Palo Alto Networks logs are considered where `event.type`, `ec.outcome` and `ec.activity` meta keys are missing. You need to create an application rule to enable these meta keys to be produced in logs. To create an application rule, see the topic [Configure Application Rules](#) in the *Decoder Configuration Guide*.

Note: Four application rules must be created and deployed for successful events, failed events, logon events, and VPN.

IMPORTANT: To ensure that UEBA always consider logon events for analytics, all of these events must contain the 8 meta keys listed above.

Ensure that you add the following VPN logs to the application rules:

1. Add success events of VPN logs to `ec.outcome = success`
2. Add failure events of VPN logs to `ec.outcome = failure`
3. Add all the authentication logon logs to `ec.activity=logon`
4. Add all the logon activity logs as `event.type=vpn`

The following figure shows four deployed application rules.

Status	Pending	Name	Condition	Session Data	Flag session with rule name in meta key	Last Updated	Severity
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ueba.auth	((reference.id = '4624';'4625';'4769';'4648') (device.type = 'ysaacsrv' AND ec.activity = 'Log...))		ueba.query	admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ueba.ad	reference.id = '4741';'4742';'4733';'4734';'4740';'4794';'5376';'5377';'5136';'4764';'4743';'4739';'...		ueba.query	admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ueba.tls	service=443 AND direction='outbound' AND analysis.service='quic' AND ip.src exists AND ip...		ueba.query	admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ueba.process	category='Process Event' AND device.type='h Wendpoint'		ueba.query	admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ueba.registry	category='Registry Event' AND device.type='h Wendpoint'		ueba.query	admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ueba.file	reference.id = '4663';'4660';'4670';'5145'		ueba.query	admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	success	device.type = 'paloaltonetworks' && result = 'success'		ec.outcome	admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	failure	device.type = 'paloaltonetworks' && result = 'failure'		ec.outcome	admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	logon	device.type = 'paloaltonetworks' && (result = 'failure' result = 'success')		ec.activity	admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	vpn	device.type = 'paloaltonetworks' && ec.activity exists && ec.outcome exists		event.type	admin	

Next steps, after completing the configuration, you can verify if UEBA is consuming the custom VPN types. For more information, see [How to verify if UEBA is consuming the Custom VPN types](#).

How to verify if UEBA is consuming the Custom VPN types

There are two ways to verify if UEBA is consuming custom VPN types.

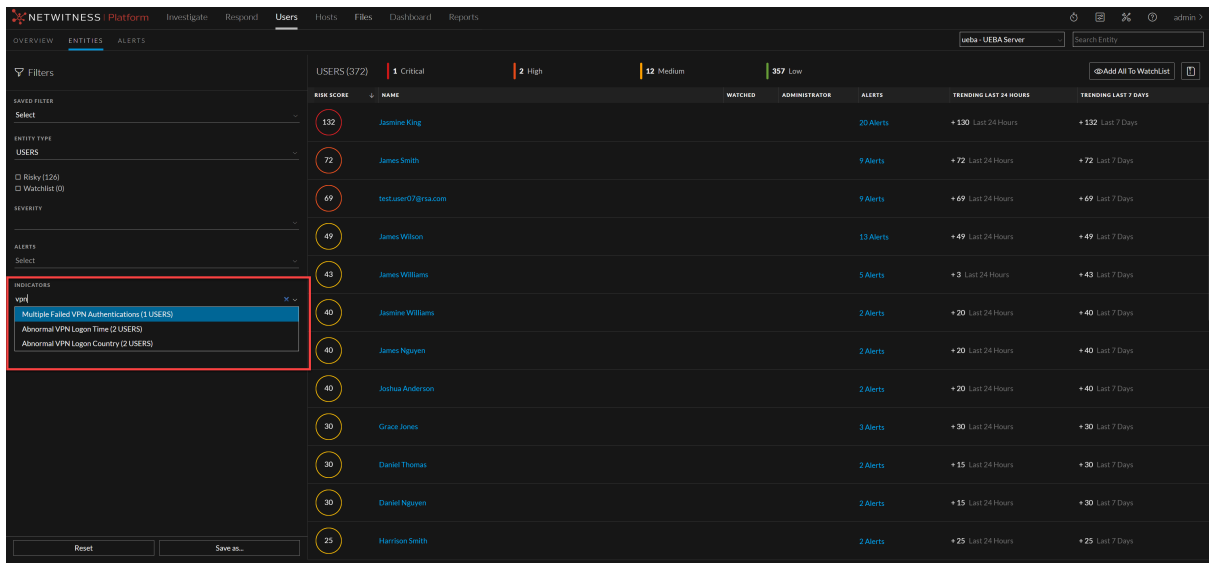
- [Using NetWitness UI](#)
- [Using the Mongo DB server](#)

Using NetWitness UI

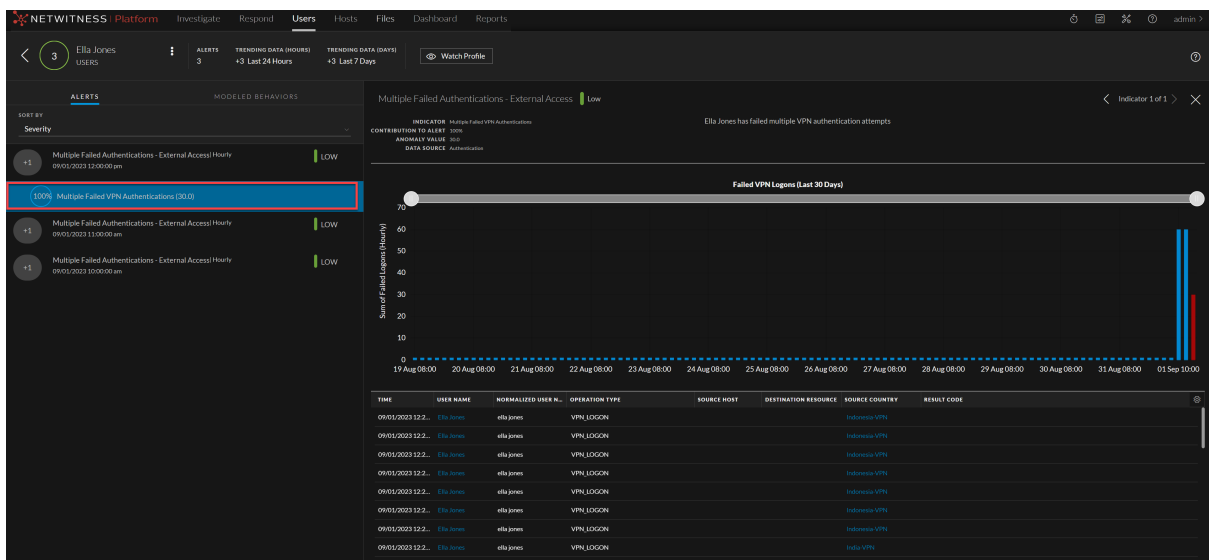
The UEBA alert can be used to confirm that the events of a custom device type are being consumed.

Note: This method is dependent on having relevant alerts that will be triggered by NetWitness UEBA.

1. Log in to the NetWitness Platform.
2. Go to **Users > Entities**.
3. In the **Filters** panel, under **Indicators**, search for a VPN indicator. For example, **Multiple Failed VPN Authentications**.

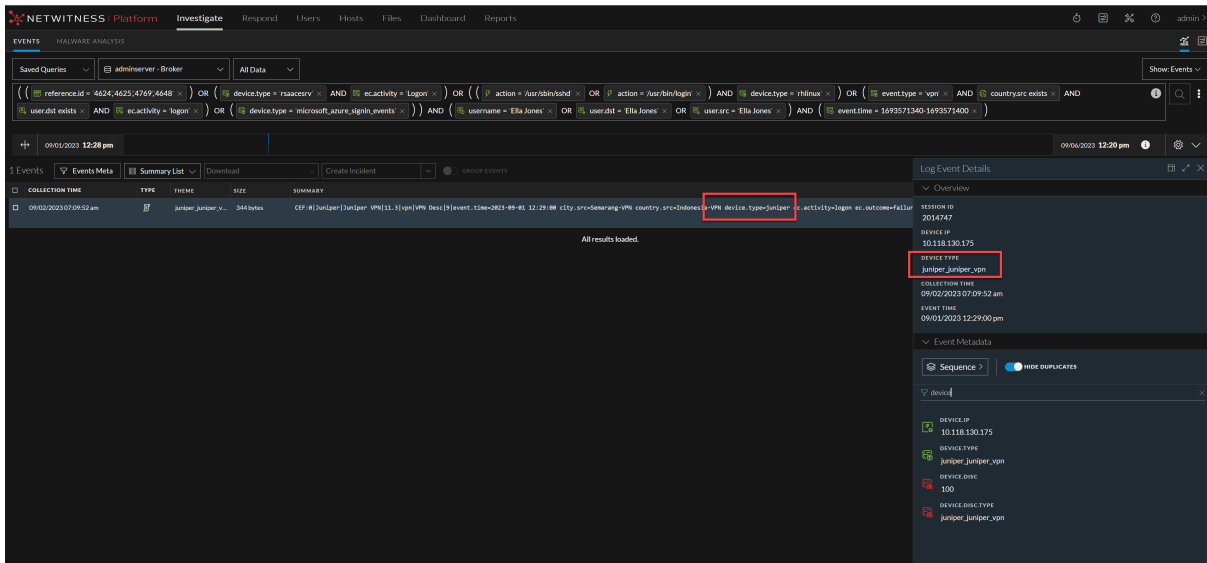


4. Click an entity name.
Indicators are displayed under the alert.
5. Select an indicator of interest.



Values that can be used to pivot are highlighted in light blue at the bottom of the panel.

6. In the Events table, click the link highlighted in blue and pivot to the alert in the Events view.
The **Investigate > Events** view is displayed.



Using the Mongo DB server

1. SSH to the UEBA server.
2. Connect to Mongo DB by running the following command:

```
mongo admin -u <user_name> -p <password>
```

Replace with your username and password for <user_name>, <password>
3. Run the following presidio command:

```
use presidio
```
4. Run the following command to get the list of devices:

```
db.output_authentication_enriched_events.distinct("datasource")
```

The events that UEBA is currently processing can be found in the list provided.

```
[
"/usr/bin/login",
"/usr/sbin/sshd",
"4624",
"4625",
"4648" ,
"azure",
"azuremonitor",
"juniper_juniper_vpn"
]
```

Note: The list includes a Juniper VPN. The list of VPNs will vary based on the environment's configuration.

UEBA Configuration

This topic provides the high-level tasks required to configure UEBA.

IMPORTANT: Changing the UEBA start-date or the UEBA processed schemas requires a re-run of the UEBA system as well as cleanup of the UEBA databases. In order to avoid deleting the information in the UI, you can use the `reset_presidio.py` script as described in [reset-presidio script](#), it will keep the data in the UI (e.g. Alerts, Indicators, Entities and Scores).

Note: To configure a single UEBA server, see "Task 3. Install and Configure NetWitness UEBA" under Installation Tasks topic in the *UEBA Standalone Installation Guide*.

Configure Multiple UEBA Servers

NetWitness Platform now supports installing multiple servers of UEBA in your environment.

Before using this feature, ensure that you meet the following requirements:

The multiple UEBA deployments are independent, with one supporting Logs & Endpoint models and the other dedicated exclusively to Network (TLS) models. Customers with a different use case will need to contact the [NetWitness Customer Support](#) team.

Multi-UEBA can be used for the following scenario:

- Multi-UEBA can only be used if there is no need for correlation between the data consumed by both UEBA servers, such as one server for Logs and Endpoint and one server for Network.

IMPORTANT: NetWitness recommends that you configure Authentication, File, Active Directory, Process, and Registry schemas on one UEBA server and TLS schema on another UEBA server for better data processing.

Prerequisites

Ensure that the NetWitness Platform and Hosts (UEBA) are in version 12.3 or later.

Procedure

1. Follow the install instructions for installing multiple UEBA servers. For example, UEBA-Server-1 and UEBA-Server-2. For more information, see "Task 3. Install and Configure NetWitness UEBA" under Installation Tasks topic in the *UEBA Standalone Installation Guide*.

Note: You can configure multiple UEBA servers in your environment. NetWitness has installed and verified up to three UEBA servers.

2. Follow the `ueba-server-config` script to set up data schemas on the installed UEBA server 1 and UEBA server 2. For more information, see [ueba-server-config script](#).

Best Practices to Add and Remove Schemas for Multiple UEBA Servers

If you are planning to install multiple UEBA servers in your environment. Consider that you have all six schemas configured in the 12.2 or an earlier version of the UEBA server.

NetWitness recommends that the TLS schema (Network data) must be configured on the new UEBA Server first, and then the existing UEBA server containing all schemas must be reset and re-configured with the five schemas Authentication, File, Active Directory, Process, and Registry (Logs and Endpoint data). For more information on configuration, see [ueba-server-config script](#). You need to reset the start date as well and ensure you set the start date one month back from the current date. For more information, see [reset-presidio script](#).

ueba-server-config script

The `ueba-server-config` script is usually used to configure and run the UEBA component after the deployment. Also, it can be used to update the UEBA configuration during run time.

IMPORTANT: If you change the start-time or the processing schemas, you must re-run UEBA. All script arguments (except the boolean arguments) are mandatory and must be filled.

For more information on the script parameters, see the *NetWitness Standalone Installation Guide for Version 12.4*.

To run the script use the following command `/opt/rsa/saTools/bin/ueba-server-config --help`

Argument	Variable	Description
-u	<user>	User name of the credentials for the Broker or Concentrator instance that you are using as a data source.
-p	<password>	<p>Password of the credentials for the Broker or Concentrator instance that you are using as a data source. The following special characters are supported in a password.</p> <pre>!"#\$%&()*+,-:;<=>?@[\\]^_`{ }</pre> <p>If you want to include a special character or special characters, you must delimit the password with an apostrophe sign, for example:</p> <pre>sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p '! "UHfz?@ExMn#\$' -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_DIRECTORY TLS PROCESS REGISTRY' -o broker -v</pre>
-h	<host>	IP address of the Broker or Concentrator used as the data source. Currently, only one data source is supported.
-o	<type>	Data source host type (broker or concentrator).

Argument	Variable	Description
-t	<startTime>	Historical start time as of which you start collecting data from the data source in YYYY-MM-DDTHH-MM-SSZ format (for example, 2018-08-15T00:00:00Z). Note: The script interprets the time you enter as UTC (Coordinated Universal Time) and it does not adjust the time to your local time zone.
-s	<schemas>	Array of data schemas. If you want to specify multiple schemas, use a space to separate each schema (for example, AUTHENTICATION FILE ACTIVE_DIRECTORY PROCESS REGISTRY TLS).
-v		verbose mode.
-e	<argument>	Boolean Argument. This enables the UEBA indicator forwarder to Respond. Note: If your NetWitness deployment includes an active Respond server, you can transfer NetWitness UEBA indicators to the Respond server and create incidents by enabling the indicator forwarder, from this data. For more information on how to enable the NetWitness UEBA incidents aggregation, see Enable User Entity Behavior Analytics Incident Rule .

Note: The TLS packet requires adding the hunting package. For more information, see [Add Features for UEBA Packet Schema](#).

reset-presidio script

IMPORTANT: The reset_presidio.py script deletes the UEBA back-end databases and can also delete the front-end database that is present in the UI.

The reset_presidio.py script is used to re-run the UEBA system as well as to update the UEBA start-date and the processing schemas easily without having to provide all the other parameters required by the ueba-server-config script. This script re-runs the UEBA while it deletes the backed data (models, aggregations, etc.). To delete the front-end data (UI entities and alerts, etc.) use the clean option. If you don't specify a date, the script will set the default start date, a 28 days earlier than the current date. NetWitness recommends that the UEBA start date is set to 28 days earlier than the current date. For UEBA systems that intend to process TLS data, you must verify that the start date is set to no later than 14 days earlier than the current date.

Note: UEBA requires to process 28 days of data before the alerts can be created.

- If you choose a start date that is less than 28 days before the current date, for example 10 days earlier from the current date, you will have to wait for another 18 days from the current date to see alerts in your UEBA system (if created).
- If you choose a start date that is greater than 27 days, it's recommended to delete the front-end database as well (use the -c) to avoid duplicate alerts.

To run the script, load the Airflow virtual environment variables as follows:

1. `source /etc/sysconfig/airflow`
2. `source $AIRFLOW_VENV/bin/activate`
3. `python /var/netwitness/presidio/airflow/venv39/lib/python3.9/site-packages/presidio_workflows-1.0-py3.9.egg/presidio/utils/airflow/reset_presidio.py --help`
4. `deactivate`

Argument	Variable	Description
-h, --help		Script Help
-c, --clean	<argument>	Clean any existing data in Elasticsearch DB (as Alerts, Indicators, Entities, etc), all data will be deleted form the UEBA UI
-s	<schema>	Reconfigure the UEBA engine array of schemas (e.g. [AUTHENTICATION FILE ACTIVE_DIRECTORY PROCESS REGISTRY TLS])
-d	<date>	Reconfigure the UEBA engine to start from midnight UTC of this date. If not set, by default reset the start date to 27 days before the current system day, at midnight UTC, to avoid duplicate alerts in the UEBA UI, in case you didn't cleaned the elasticsearch data (-c) (e.g. 2010-12-31)

Please refer to the above table for the required arguments to pass along with the reset command. For more information, refer to the example command below.

```
python /var/netwitness/presidio/airflow/venv39/lib/python3.9/site-packages/presidio_workflows-1.0-py3.9.egg/presidio/utils/airflow/reset_presidio.py -c -d 2023-11-16 -s AUTHENTICATION ACTIVE_DIRECTORY FILE PROCESS REGISTRY TLS
```

Add a Schema without Rerunning the UEBA

Note: Adding a schema without rerunning the UEBA system is supported on NetWitness Platform 11.5.1 and later.

To add a new UEBA schema without rerunning the UEBA system, run the following command on the UEBA host.

```
curl -X PATCH http://localhost:8881/configuration -H 'content-type: application/json' -d '{"operations": [{"op": "add", "path": "/dataPipeline/schemas/-", "value": "<SCHEMA>"}]}'
```

Where <SCHEMA> string can be replaced with any one of the following schemas:

- AUTHENTICATION
- FILE
- ACTIVE_DIRECTORY

- PROCESS
- REGISTRY
- TLS

UEBA Indicator Forwarder

Note: The UEBA Indicator Forwarder is supported by the UEBA from version 11.3 and later. If your NetWitness environment includes an active respond server, you can transfer the UEBA indicators to the respond server and to the correlation server in order to create Incidents. For more information, see [Enable User Entity Behavior Analytics Incident Rule](#).

Run the following command to activate the UEBA Indicator Forwarder:

```
curl -X PATCH http://localhost:8881/configuration -H 'content-type: application/json' -d '{"operations": [{"op": "replace", "path": "/outputForwarding/enableForwarding", "value": true}]}'
```

To deactivate the UEBA indicator forwarder, change the “value”:true at the request body to be “value”:false.

Update Data Source Details

In order to update the details of the data source you must use the `ueba-server-config` script. For more information, see [ueba-server-config script](#).

Note: From 12.3 version or later, if you change the data source using the [ueba-server-config script](#), UEBA will use the previously configured start date by default. To change the UEBA start date, use the [reset-presidio script](#).


The data sources details are:

- Data Source type (Broker / Concentrator).
- Data Source username.
- Data Source password.
- Data Source host.

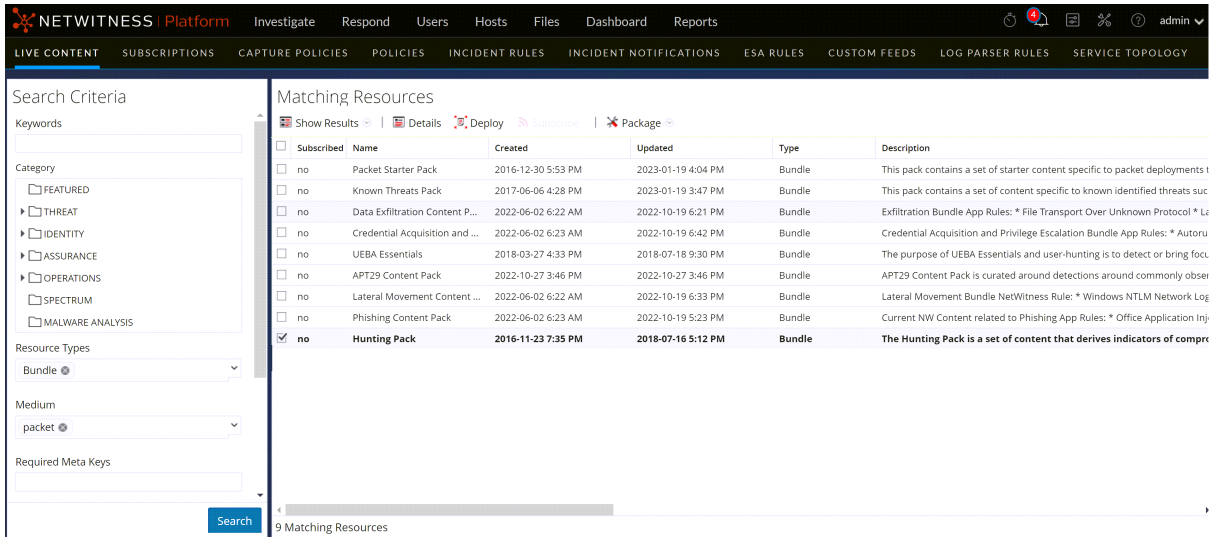
Add Features for UEBA Packet Schema

Add the Hunting Pack:

In NetWitness Platform, add the hunting pack or verify it’s available:

1. Log in to the NetWitness Platform.
2. Navigate to  (Admin) and select **Admin Server**.

- Click  and select **Configure > Live Content**.



The screenshot shows the NetWitness Platform interface for configuring Live Content. The top navigation bar includes 'NETWITNESS | Platform' and various tabs like 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. Below the navigation bar, there are several sub-tabs: 'LIVE CONTENT', 'SUBSCRIPTIONS', 'CAPTURE POLICIES', 'POLICIES', 'INCIDENT RULES', 'INCIDENT NOTIFICATIONS', 'ESA RULES', 'CUSTOM FEEDS', 'LOG PARSER RULES', and 'SERVICE TOPOLOGY'. The 'LIVE CONTENT' tab is active.

The interface is split into two main sections: 'Search Criteria' on the left and 'Matching Resources' on the right.

Search Criteria:

- Keywords:** A text input field.
- Category:** A tree view showing categories: FEATURED, THREAT, IDENTITY, ASSURANCE, OPERATIONS, SPECTRUM, and MALWARE ANALYSIS.
- Resource Types:** A dropdown menu set to 'Bundle'.
- Medium:** A dropdown menu set to 'packet'.
- Required Meta Keys:** A text input field.
- Search:** A blue button at the bottom of the search criteria section.

Matching Resources:

At the top of this section, there are action buttons: 'Show Results', 'Details', 'Deploy', 'Subscribe', and 'Package'. Below these is a table with 9 rows of resources. The 'Hunting Pack' row is selected, and the 'Deploy' button is highlighted.


Subscribed	Name	Created	Updated	Type	Description
<input type="checkbox"/>	Packet Starter Pack	2016-12-30 5:53 PM	2023-01-19 4:04 PM	Bundle	This pack contains a set of starter content specific to packet deployments t
<input type="checkbox"/>	Known Threats Pack	2017-06-06 4:28 PM	2023-01-19 3:47 PM	Bundle	This pack contains a set of content specific to known identified threats suc
<input type="checkbox"/>	Data Exfiltration Content P...	2022-06-02 6:22 AM	2022-10-19 6:21 PM	Bundle	Exfiltration Bundle App Rules: * File Transport Over Unknown Protocol * Li
<input type="checkbox"/>	Credential Acquisition and ...	2022-06-02 6:23 AM	2022-10-19 6:42 PM	Bundle	Credential Acquisition and Privilege Escalation Bundle App Rules: * Aтору
<input type="checkbox"/>	UEBA Essentials	2018-03-27 4:33 PM	2018-07-18 9:30 PM	Bundle	The purpose of UEBA Essentials and user-hunting is to detect or bring focu
<input type="checkbox"/>	APT29 Content Pack	2022-10-27 3:46 PM	2022-10-27 3:46 PM	Bundle	APT29 Content Pack is curated around detections around commonly obser
<input type="checkbox"/>	Lateral Movement Content ...	2022-06-02 6:22 AM	2022-10-19 6:33 PM	Bundle	Lateral Movement Bundle NetWitness Rule: * Windows NTLM Network Log
<input type="checkbox"/>	Phishing Content Pack	2022-06-02 6:23 AM	2022-10-19 5:23 PM	Bundle	Current NW Content related to Phishing App Rules: * Office Application Inj
<input checked="" type="checkbox"/>	Hunting Pack	2016-11-23 7:35 PM	2018-07-16 5:12 PM	Bundle	The Hunting Pack is a set of content that derives indicators of compr

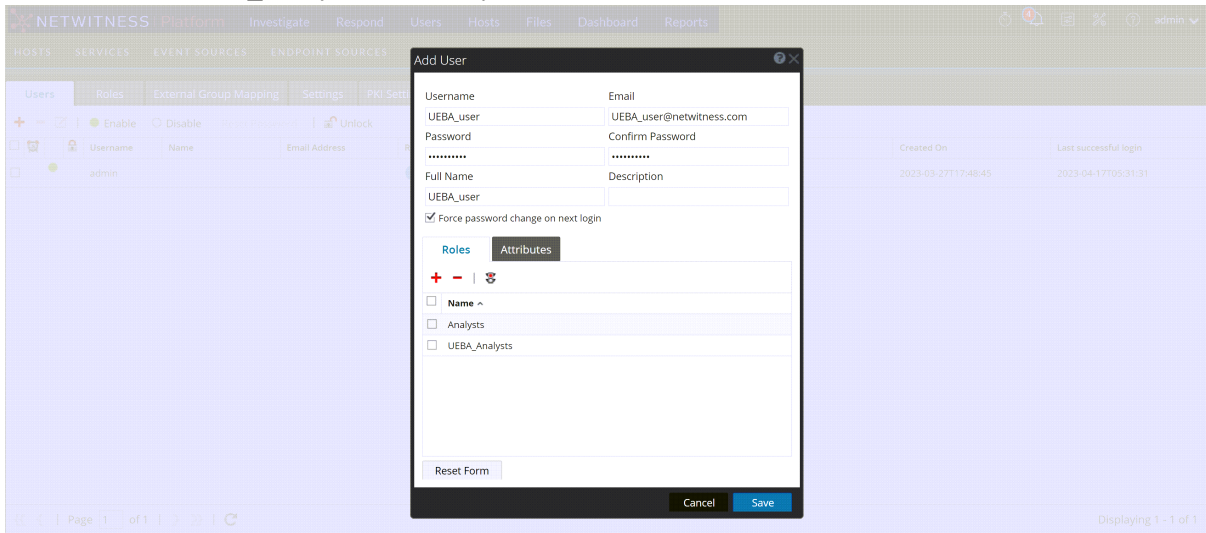
At the bottom of the 'Matching Resources' section, there is a 'Search' button and a status indicator '9 Matching Resources'.

- On the left menu, select the following:
 - Bundle under Resources Type.
 - Packet under Medium
- Click **Search**.
A list of matching resources is displayed.
- Select **Hunting Pack** from the list and click **Deploy**.
The hunting pack is added.

Assign User Access to UEBA

To create a user with privileges to access the UEBA pages (Users tab) on the Netwitness UI do the following:


1. Navigate to  (Admin) > **Security**.
2. Create a new UEBA_Analysts and Analysts user roles.



For more information, see the "Manage Users with Roles and Permissions" topic in the *System Security and User Management Guide*.

Create an Analysts Role

In order to fetch data from the data source (Broker / Concentrator), you need to create a user using the Analysts role in the data source service.

1. Navigate to the security tab at the data source service page.
2. Go to the  (Admin) > **Services** > **Security**.

3. Create an analyst user and assign it to the any of supported special characters.

The screenshot shows the NetWitness Platform user configuration page for a user named 'uebauser'. The interface is divided into several sections:


- User Information:** Fields for Name (Ueba User), Username (uebauser), Password, Confirm Password, Email (ueba.user@rsa.com), and Description.
- User Settings:** Fields for Auth Type (NetWitness Platform), Core Query Timeout (60), Query Prefix, and Session Threshold (0).
- Role Membership:** A list of roles with checkboxes. The 'Analysts' role is selected, while others like Administrators, Aggregation, Data_Privacy_Officers, Malware_Analysts, Operators, and SOC_Managers are not.

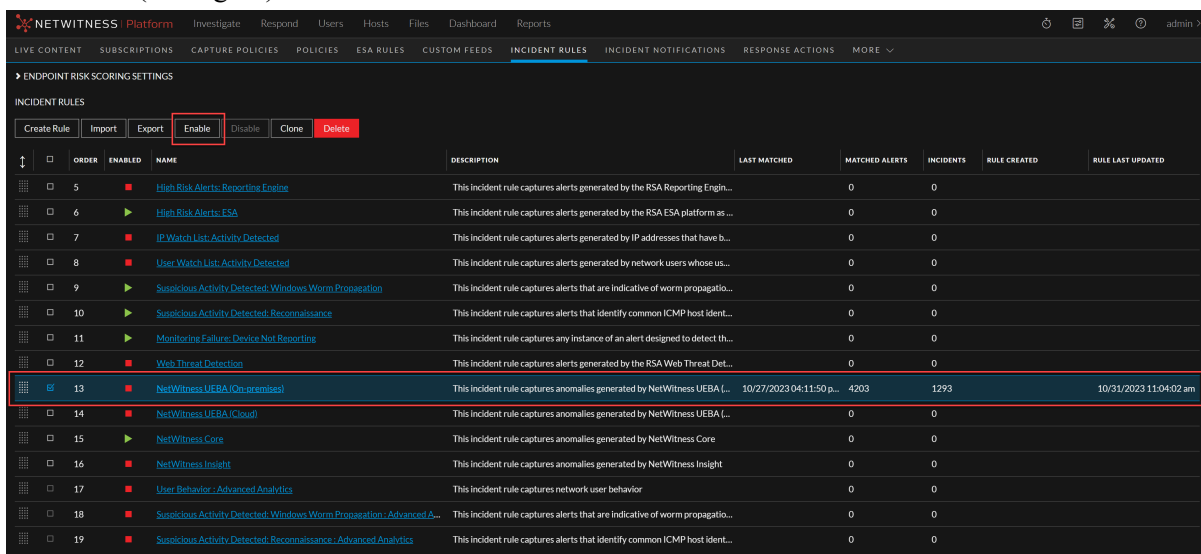
Enable User Entity Behavior Analytics Incident Rule

In order to aggregate the UEBA indicators under Incident rule, follow the instructions below:

Enable the UEBA Forwarding process as described in [Enable UEBA Indicator Forwarder](#).

Note: By default, the NetWitness UEBA (On-premises) rules are disabled in your environment. You can enable them to generate the incident IDs for the alerts and customize the NetWitness UEBA (On-premises) rules settings.

1. Go to  (Configure) > **Incident Rules**.



2. Select the **NetWitness UEBA (On-premises)** rule and click **Enable**. A confirmation pop-up is displayed.
3. Click **OK**.

Enable or Disable Modeled Behaviors for Users

The UEBA Modeled Behaviors functionality is enabled by default from version 11.5.1.

To disable perform the following:

1. SSH to the UEBA server.

Edit and add the parameter `entity.profile.enabled=false` in the file `/etc/netwitness/presidio/configserver/configurations/presidio-uiconf.properties`.

2. Run the command to restart the `presidio-ui`.

```
systemctl restart presidio-ui
```

Note: To enable, remove the parameter `entity.profile.enabled=false` from the file and restart the `presidio-ui` using the step 2.

Once you have enabled or disabled the Modeled Behaviors, you can verify from NetWitness Platform UI.

To verify, perform the following:

- a. Log in to the NetWitness Platform and click **Users**.
- b. In the **Overview** tab, under **Top Risky Users** panel, click on a username.

- c. Click the **Modeled Behaviors** tab.
For more information, see "View Modeled Behaviors" topic in the *UEBA User Guide for NetWitness Platform 12.3*.

Removal of Packetbeat Service

From the 12.3 version or later, the Packbeat service has been removed from UEBA to improve memory usage and performance. This allows other services in UEBA to utilize the resources more efficiently, reducing the load on the system.

Learning Period Per Scale

Learning Period Per Scale for 12.4

Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<ul style="list-style-type: none"> • Scale 1: 125,000 users with 40 million Log and Endpoint events + 60 million Network events with 100,000 JA3 entities per day • Scale 2: 150,000 users with 50 million Log and Endpoint events + 70 million Network events with 150,000 JA3 entities per day 	Yes	<p>Fresh Installation of 12.4</p> <ul style="list-style-type: none"> • Scale 1: Up to 6.5 days with 28 days of historical data • Scale 2: Up to 9 days with 28 days of historical data
<ul style="list-style-type: none"> • Scale 1: 125,000 users with 40 million Log and Endpoint events + 60 million Network events with 100,000 JA3 entities per day • Scale 2: 150,000 users with 50 million Log and Endpoint events + 70 million Network events with 150,000 JA3 entities per day 	Yes	<p>Upgrade from 12.2.x, 12.3, 12.3.1 to 12.4</p> <p>UEBA reset is not required.</p> <ul style="list-style-type: none"> • If learning period is already completed, data will be processed for alert generation immediately. • If learning period is completed only for N days, then it will take 28-N days to complete the learning period before generating alerts.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<ul style="list-style-type: none"> • Scale 1: 125,000 users with 40 million Log and Endpoint events + 60 million Network events with 100,000 JA3 entities per day • Scale 2: 150,000 users with 50 million Log and Endpoint events + 70 million Network events with 150,000 JA3 entities per day 	Yes	<p>Upgrade from 12.2.x, 12.3, 12.3.1 to 12.4 with schemas updated (Addition or removal of schemas configured on UEBA)</p> <p>UEBA reset is required.</p> <p>Historical data is available for N days:</p> <ul style="list-style-type: none"> • Scale 1 with N > 28 days : Up to 6.5 days with 28 days of historical data. • Scale 2 with N > 28 days: Up to 9 days with 28 days of historical data • Scale 1 and Scale 2 with N < 28 days: It will take 28-N days to complete the learning period before generating alerts. <p>Historical data is not available</p> <p>28 days to complete the learning period before generating alerts.</p>
<ul style="list-style-type: none"> • Scale 1: 125,000 users with 40 million Log and Endpoint events + 60 million Network events with 100,000 JA3 entities per day • Scale 2: 150,000 users with 50 million Log and Endpoint events + 70 million Network events with 150,000 JA3 entities per day 	No	<p>Fresh installation of 12.4</p> <p>28 days to complete the learning period before generating alerts.</p>

Virtual Machine

The recommended vCPU specification for UEBA is Intel Xeon CPU @2.59 Ghz.

CPU	Memory	Reserved Memory Allocation	Disk Requirements for /var/netwitness Partition	Read IOPS	Write IOPS
32 cores	256GB	192GB	<ul style="list-style-type: none"> Storage: 1.5 TB Provisioning: Thick 	500	500

To determine the scale limits for Virtual Machine deployments, refer to the **Scaling Limitation Issue** section in the [Troubleshooting UEBA Configurations](#).

IMPORTANT:

- You must reserve all the resources allocated to UEBA on the VM server. For example, if a user has a 2.1GHz CPU, then 32CPUs * 2.1GHz = 67.2GHz or 67200MHz must be reserved.
- The /var/netwitness partition must be mounted on a **1.5 TB** Thick-provisioned disk for storage usage.

Note: NetWitness recommends you to deploy UEBA on a virtual host, only if your log collection volume is low. If you have a moderate to high log collection volume, NetWitness recommends you to deploy UEBA on the physical host as described in the "NetWitness UEBA Host Hardware Specifications" topic of the *Physical Host Installation Guide*. Contact NetWitness Customer Support (<https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897>) for advice on choosing which host, virtual or physical, to use for UEBA.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<ul style="list-style-type: none"> • Scale 1: 125,000 users with 40 million Log and Endpoint events + 20 million Network events with 100,000 JA3 entities per day • Scale 2: 150,000 users with 50 million Log and Endpoint events + 25 million Network events with 150,000 JA3 entities per day 	Yes	<p>Fresh Installation of 12.4</p> <ul style="list-style-type: none"> • Scale 1: Up to 6.5 days with 28 days of historical data • Scale 2: Up to 7.5 days with 28 days of historical data

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<ul style="list-style-type: none"> • Scale 1: 125,000 users with 40 million Log and Endpoint events + 20 million Network events with 100,000 JA3 entities per day • Scale 2: 150,000 users with 50 million Log and Endpoint events + 25 million Network events with 150,000 JA3 entities per day 	Yes	<p>Upgrade from 12.2.x, 12.3, 12.3.1 to 12.4</p> <p>UEBA reset is not required.</p> <ul style="list-style-type: none"> • If learning period is already completed, data will be processed for alert generation immediately. • If learning period is completed only for N days, then it will take 28-N days to complete the learning period before generating alerts .

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<ul style="list-style-type: none"> • Scale 1: 125,000 users with 40 million Log and Endpoint events + 20 million Network events with 100,000 JA3 entities per day • Scale 2: 150,000 users with 50 million Log and Endpoint events + 25 million Network events with 150,000 JA3 entities per day 	Yes	<p>Upgrade from 12.2.x, 12.3, 12.3.1 to 12.4 with schemas updated (Addition or removal of schemas configured on UEBA)</p> <p>UEBA reset is required.</p> <p>Historical data is available for N days:</p> <ul style="list-style-type: none"> • Scale 1 with $N > 28$ days: Up to 6.5 days with 28 days of historical data. • Scale 2 with $N > 28$ days: Up to 7.5 days with 28 days of historical data. • Scale 1 and Scale 2 with $N < 28$ days: It will take $28-N$ days to complete the learning period before generating alerts. <p>Historical data is not available</p> <p>28 days to complete the learning period before generating alerts.</p>
<ul style="list-style-type: none"> • Scale 1: 125,000 users with 40 million Log and Endpoint events + 20 million Network events with 100,000 JA3 entities per day • Scale 2: 150,000 users with 50 million Log and Endpoint events + 25 million Network events with 150,000 JA3 entities per day 	No	<p>Fresh installation of 12.4</p> <p>28 days to complete the learning period before generating alerts.</p>

Note: Network events per day refers to number of events consumed by UEBA per day.

Learning Period Per Scale for 12.4 Multiple UEBA Servers

Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)

Note: There are two UEBA servers, one is configured with Log and Endpoint data, while the other is configured with Network (TLS) data.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period <small>Alerts will be generated when the learning period is complete</small>
<p>Scale 1 for Multi-UEBA:</p> <ul style="list-style-type: none"> • UEBA Server 1: 125,000 users with 120 million Log and Endpoint events per day • UEBA Server 2: 100 million Network events with 100,000 JA3 entities per day <p>Scale 2 for Multi-UEBA:</p> <ul style="list-style-type: none"> • UEBA Server 1: 200,000 users with 150 million Log and Endpoint events per day • UEBA Server 2: 110 million Network events with 150,000 JA3 entities per day 	<p>Yes</p>	<p>Fresh Installation of 12.4</p> <ul style="list-style-type: none"> • Scale 1: Up to 8.5 days with 28 days of historical data • Scale 2: Up to 12 days with 28 days of historical data

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<p>Scale 1 for Multi-UEBA:</p> <ul style="list-style-type: none"> • UEBA Server 1: 125,000 users with 120 million Log and Endpoint events per day • UEBA Server 2: 100 million Network events with 100,000 JA3 entities per day <p>Scale 2 for Multi-UEBA:</p> <ul style="list-style-type: none"> • UEBA Server 1: 200,000 users with 150 million Log and Endpoint events per day • UEBA Server 2: 110 million Network events with 150,000 JA3 entities per day 	<p>Yes</p>	<p>Upgrade from 12.2.x, 12.3, 12.3.1 to 12.4</p> <p>UEBA reset is not required.</p> <ul style="list-style-type: none"> • If learning period is already completed, data will be processed for alert generation immediately. • If learning period is completed only for N days, then it will take 28-N days to complete the learning period before generating alerts.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<p>Scale 1 for Multi-UEBA:</p> <ul style="list-style-type: none"> • UEBA Server 1: 125,000 users with 120 million Log and Endpoint events per day • UEBA Server 2: 100 million Network events with 100,000 JA3 entities per day <p>Scale 2 for Multi-UEBA:</p> <ul style="list-style-type: none"> • UEBA Server 1: 200,000 users with 150 million Log and Endpoint events per day • UEBA Server 2: 110 million Network events with 150,000 JA3 entities per day 	<p>Yes</p>	<div style="border: 1px solid green; padding: 5px;"> <p>Note: An additional UEBA server must be installed to configure TLS schema on a separate UEBA server. For example, if you are planning to upgrade from 12.2:</p> <p>Before upgrade: UEBA Server 1 is configured with Log, Endpoint, and TLS data.</p> <p>After upgrade:</p> <ul style="list-style-type: none"> • Add another UEBA Server 2 and configure it with TLS schema. • Reconfigure UEBA Server 1 with only Log and Endpoint data followed by UEBA reset. <p>For more information, see Best Practices to Add and Remove Schemas for Multiple UEBA Servers.</p> </div> <p>Upgrade from 12.2.x, 12.3, 12.3.1 to 12.4 with schemas updated (Addition or removal of schemas configured on UEBA)</p> <p>UEBA reset is required.</p> <p>Historical data is available for N days:</p> <ul style="list-style-type: none"> • Scale 1 with N > 28 days: Up to 8.5 days with 28 days of historical data. • Scale 2 with N > 28 days: Up to 12 days with 28 days of historical data. • Scale 1 and Scale 2 with N < 28 days: It will take 28-N days to complete the learning period before generating alerts. <p>Historical data is not available</p> <p>28 days to complete the learning period before generating alerts.</p>

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<p>Scale 1 for Multi-UEBA:</p> <ul style="list-style-type: none"> • UEBA Server 1: 125,000 users with 120 million Log and Endpoint events per day • UEBA Server 2: 100 million Network events with 100,000 JA3 entities per day <p>Scale 2 for Multi-UEBA:</p> <ul style="list-style-type: none"> • UEBA Server 1: 200,000 users with 150 million Log and Endpoint events per day • UEBA Server 2: 110 million Network events with 150,000 JA3 entities per day 	No	<p>Fresh installation of 12.4</p> <p>28 days to complete the learning period before generating alerts.</p>

Learning Period Per Scale for 12.3.1

Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
125,000 users with 40 million Log and Endpoint events + 60 million Network events with 100,000 JA3 entities per day	Yes	<p>Fresh Installation of 12.3.1</p> <p>Up to 12 days with 28 days of historical data</p>

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
125,000 users with 40 million Log and Endpoint events + 60 million Network events with 100,000 JA3 entities per day	Yes	<p>Upgrade from 11.7.x, 12.1.x, 12.2.x, 12.3 to 12.3.1</p> <p>UEBA reset is not required.</p> <ul style="list-style-type: none"> • If learning period is already completed, data will be processed for alert generation immediately. • If learning period is completed only for N days, then it will take 28-N days to complete the learning period before generating alerts.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
125,000 users with 40 million Log and Endpoint events + 60 million Network events with 100,000 JA3 entities per day	Yes	<p>Upgrade from 11.7.x, 12.1.x, 12.2.x, 12.3 to 12.3.1 with schemas updated (Addition or removal of schemas configured on UEBA)</p> <p>UEBA reset is required.</p> <p>Historical data is available for N days:</p> <ul style="list-style-type: none"> • N > 28 days: Up to 12 days with 28 days of historical data. • N < 28 days: It will take 28-N days to complete the learning period before generating alerts. <p>Historical data is not available</p> <p>28 days to complete the learning period before generating alerts.</p>

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
125,000 users with 40 million Log and Endpoint events + 60 million Network events with 100,000 JA3 entities per day	No	Fresh installation of 12.3.1 28 days to complete the learning period before generating alerts.

Virtual Machine

The recommended vCPU specification for UEBA is Intel Xeon CPU @2.59 Ghz.

CPU	Memory	Reserved Memory Allocation	Disk Requirements for /var/netwitness Partition	Read IOPS	Write IOPS
32 cores	256GB	192GB	<ul style="list-style-type: none"> Storage: 1.5 TB Provisioning: Thick 	500	500

To determine the scale limits for Virtual Machine deployments, refer to the **Scaling Limitation Issue** section in the [Troubleshooting UEBA Configurations](#).

IMPORTANT:

- You must reserve all the resources allocated to UEBA on the VM server. For example, if a user has a 2.1GHz CPU, then 32CPUs * 2.1GHz = 67.2GHz or 67200MHz must be reserved.
- The **/var/netwitness** partition must be mounted on a **1.5 TB** Thick-provisioned disk for storage usage.

Note: NetWitness recommends you to deploy UEBA on a virtual host, only if your log collection volume is low. If you have a moderate to high log collection volume, NetWitness recommends you to deploy UEBA on the physical host as described in the "NetWitness UEBA Host Hardware Specifications" topic of the *Physical Host Installation Guide*. Contact NetWitness Customer Support (<https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897>) for advice on choosing which host, virtual or physical, to use for UEBA.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
125,000 users with 40 million Log and Endpoint events + 20 million Network events with 100,000 JA3 entities per day	Yes	Fresh Installation of 12.3.1 Up to 10 days with 28 days of historical data
125,000 users with 40 million Log and Endpoint events + 20 million Network events with 100,000 JA3 entities per day	Yes	Upgrade from 11.7.x, 12.1.x, 12.2.x, 12.3 to 12.3.1 UEBA reset is not required. <ul style="list-style-type: none"> • If learning period is already completed, data will be processed for alert generation immediately. • If learning period is completed only for N days, then it will take 28-N days to complete the learning period before generating alerts .

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
125,000 users with 40 million Log and Endpoint events + 20 million Network events with 100,000 JA3 entities per day	Yes	<p>Upgrade from 11.7.x, 12.1.x, 12.2.x, 12.3 to 12.3.1 with schemas updated (Addition or removal of schemas configured on UEBA)</p> <p>UEBA reset is required.</p> <p>Historical data is available for N days:</p> <ul style="list-style-type: none"> • N > 28 days: Up to 10 days with 28 days of historical data. • N < 28 days: It will take 28-N days to complete the learning period before generating alerts. <p>Historical data is not available</p> <p>28 days to complete the learning period before generating alerts.</p>
125,000 users with 40 million Log and Endpoint events + 20 million Network events with 100,000 JA3 entities per day	No	<p>Fresh installation of 12.3.1</p> <p>28 days to complete the learning period before generating alerts.</p>

Note: Network events per day refers to number of events consumed by UEBA per day.

Learning Period Per Scale for 12.3.1 Multiple UEBA Servers

Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)

Note: There are two UEBA servers, one is configured with Log and Endpoint data, while the other is configured with Network (TLS) data.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<p>UEBA Server 1: 125,000 users with 120 million Log and Endpoint events per day</p> <p>UEBA Server 2: 100 million Network events with 100,000 JA3 entities per day</p>	<p>Yes</p>	<p>Fresh Installation of 12.3.1 Up to 12 days with 28 days of historical data</p>
<p>UEBA Server 1: 125,000 users with 120 million Log and Endpoint events per day</p> <p>UEBA Server 2: 100 million Network events with 100,000 JA3 entities per day</p>	<p>Yes</p>	<p>Upgrade from 11.7.x, 12.1.x, 12.2.x, 12.3 to 12.3.1</p> <p>UEBA reset is not required.</p> <ul style="list-style-type: none"> • If learning period is already completed, data will be processed for alert generation immediately. • If learning period is completed only for N days, then it will take 28-N days to complete the learning period before generating alerts.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<p>UEBA Server 1: 125,000 users with 120 million Log and Endpoint events per day</p> <p>UEBA Server 2: 100 million Network events with 100,000 JA3 entities per day</p>	<p>Yes</p>	<div style="border: 1px solid green; padding: 5px;"> <p>Note: An additional UEBA server must be installed to configure TLS schema on a separate UEBA server. For example, if you are planning to upgrade from 11.7.1:</p> <p>Before upgrade: UEBA Server 1 is configured with Log, Endpoint, and TLS data.</p> <p>After upgrade:</p> <ul style="list-style-type: none"> • Add another UEBA Server 2 and configure it with TLS schema. • Reconfigure UEBA Server 1 with only Log and Endpoint data followed by UEBA reset. <p>For more information, see Best Practices to Add and Remove Schemas for Multiple UEBA Servers.</p> </div> <p>Upgrade from 11.7.x, 12.1.x, 12.2.x, 12.3 to 12.3.1 with schemas updated (Addition or removal of schemas configured on UEBA)</p> <p>UEBA reset is required.</p> <p>Historical data is available for N days:</p> <ul style="list-style-type: none"> • N > 28 days: Up to 12 days with 28 days of historical data. • N < 28 days: It will take 28-N days to complete the learning period before generating alerts. <p>Historical data is not available</p> <p>28 days to complete the learning period before generating alerts.</p>

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<p>UEBA Server 1: 125,000 users with 120 million Log and Endpoint events per day</p> <p>UEBA Server 2: 100 million Network events with 100,000 JA3 entities per day</p>	No	<p>Fresh installation of 12.3.1</p> <p>28 days to complete the learning period before generating alerts.</p>

Learning Period Per Scale for 12.3

Note: The displayed numbers are with the following enhancement enabled. Ensure that you enable the configuration in the `application.properties` file to improve the processing time. For more information, see **The TLS model is taking too long to complete tasks** section in the [Troubleshooting UEBA Configurations](#).

Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
100,000 users with 30 million Log and Endpoint events + 60 million Network events per day	Yes	<p>Fresh Installation of 12.3</p> <p>Up to 10 days with 28 days of historical data</p>
100,000 users with 30 million Log and Endpoint events + 60 million Network events per day	Yes	<p>Upgrade from 11.7.x, 12.1.x, 12.2.x to 12.3</p> <p>UEBA reset is not required.</p> <ul style="list-style-type: none"> • If learning period is already completed, data will be processed for alert generation immediately. • If learning period is completed only for N days, then it will take 28-N days to complete the learning period before generating alerts.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
100,000 users with 30 million Log and Endpoint events + 60 million Network events per day	Yes	<p>Upgrade from 11.7.x, 12.1.x, 12.2.x to 12.3 with schemas updated (Addition or removal of schemas configured on UEBA)</p> <p>UEBA reset is required.</p> <p>Historical data is available for N days:</p> <ul style="list-style-type: none"> • N > 28 days: Up to 10 days with 28 days of historical data. • N < 28 days: It will take 28-N days to complete the learning period before generating alerts. <p>Historical data is not available</p> <p>28 days to complete the learning period before generating alerts.</p>
100,000 users with 30 million Log and Endpoint events + 60 million Network events per day	No	<p>Fresh installation of 12.3</p> <p>28 days to complete the learning period before generating alerts.</p>

Virtual Machine

The recommended vCPU specification for UEBA is Intel Xeon CPU @2.59 Ghz.

CPU	Memory	Reserved Memory Allocation	Disk Requirements for /var/netwitness Partition	Read IOPS	Write IOPS
32 cores	128GB	64GB	<ul style="list-style-type: none"> • Storage: 1.5 TB • Provisioning: Thick 	500	500

IMPORTANT: The /var/netwitness partition must be mounted on a **1.5 TB** Thick-provisioned disk for storage usage.

To determine the scale limits for Virtual Machine deployments, refer to the **Scaling Limitation Issue** section in the [Troubleshooting UEBA Configurations](#).

Note: NetWitness recommends you to deploy UEBA on a virtual host, only if your log collection volume is low. If you have a moderate to high log collection volume, NetWitness recommends you to deploy UEBA on the physical host as described in the "NetWitness UEBA Host Hardware Specifications" topic of the *Physical Host Installation Guide*. Contact NetWitness Customer Support (<https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897>) for advice on choosing which host, virtual or physical, to use for UEBA.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
100,000 users with 30 million Log and Endpoint events + 20 million Network events per day	Yes	Fresh Installation of 12.3 Up to 8 days with 28 days of historical data
100,000 users with 30 million Log and Endpoint events + 20 million Network events per day	Yes	Upgrade from 11.7.x, 12.1.x, 12.2.x to 12.3 UEBA reset is not required. <ul style="list-style-type: none"> • If learning period is already completed, data will be processed for alert generation immediately. • If learning period is completed only for N days, then it will take 28-N days to complete the learning period before generating alerts.
100,000 users with 30 million Log and Endpoint events + 20 million Network events per day	Yes	Upgrade from 11.7.x, 12.1.x, 12.2.x to 12.3 with schemas updated (Addition or removal of schemas configured on UEBA) UEBA reset is required. Historical data is available for N days: <ul style="list-style-type: none"> • N > 28 days: Up to 8 days with 28 days of historical data. • N < 28 days: It will take 28-N days to complete the learning period before generating alerts. Historical data is not available 28 days to complete the learning period before generating alerts.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
100,000 users with 30 million Log and Endpoint events + 20 million Network events per day	No	Fresh installation of 12.3 28 days to complete the learning period before generating alerts.

Note: Network events per day refers to number of events consumed by UEBA per day.

Learning Period Per Scale for 12.3 Multiple UEBA Servers

Physical Machine (SERIES 6 ESA (DELL R640) SPECIFICATIONS)

Note: There are two UEBA servers, one is configured with Log and Endpoint data, while the other is configured with Network (TLS) data.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<p>UEBA Server 1: 100,000 users with 100 million Log and Endpoint events per day</p> <p>UEBA Server 2: 100 million Network events per day</p>	Yes	Fresh Installation of 12.3 Up to 10 days with 28 days of historical data

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<p>UEBA Server 1: 100,000 users with 100 million Log and Endpoint events per day</p> <p>UEBA Server 2: 100 million Network events per day</p>	<p>Yes</p>	<p>Upgrade from 11.7.x, 12.1.x, 12.2.x to 12.3</p> <p>UEBA reset is not required.</p> <ul style="list-style-type: none"> • If learning period is already completed, data will be processed for alert generation immediately. • If learning period is completed only for N days, then it will take 28-N days to complete the learning period before generating alerts.
<p>UEBA Server 1: 100,000 users with 100 million Log and Endpoint events per day</p> <p>UEBA Server 2: 100 million Network events per day</p>	<p>Yes</p>	<div style="border: 1px solid green; padding: 5px;"> <p>Note: An additional UEBA server must be installed to configure TLS schema on a separate UEBA server. For example, if you are planning to upgrade from 11.7.1:</p> <p>Before upgrade: UEBA Server 1 is configured with Log, Endpoint, and TLS data.</p> <p>After upgrade:</p> <ul style="list-style-type: none"> • Add another UEBA Server 2 and configure it with TLS schema. • Reconfigure UEBA Server 1 with only Log and Endpoint data followed by UEBA reset. <p>For more information, see Best Practices to Add and Remove Schemas for Multiple UEBA Servers.</p> </div> <p>Upgrade from 11.7.x, 12.1.x, 12.2.x to 12.3 with schemas updated (Addition or removal of schemas configured on UEBA)</p> <p>UEBA reset is required.</p>

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<p>UEBA Server 1: 100,000 users with 100 million Log and Endpoint events per day</p> <p>UEBA Server 2: 100 million Network events per day</p>	Yes	<p>Historical data is available for N days:</p> <ul style="list-style-type: none"> • N > 28 days: Up to 10 days with 28 days of historical data. • N < 28 days: It will take 28-N days to complete the learning period before generating alerts. <p>Historical data is not available 28 days to complete the learning period before generating alerts.</p>
<p>UEBA Server 1: 100,000 users with 100 million Log and Endpoint events per day</p> <p>UEBA Server 2: 50 million Network events per day</p>	No	<p>Fresh installation of 12.3 28 days to complete the learning period before generating alerts.</p>

Learning Period Per Scale (from 11.5.1 version to 12.2.0.1)

Note: For all supported scales, when historical data is not available, the learning period is 28 days.

Physical Machine

SERIES 5 (DELL R630) SPECIFICATIONS

Supported Scale for existing NetWitness customers (historical data is available)	Learning Period Alerts will be generated when the learning period is complete
<p>Logs and Endpoint data for 100,000 users with 30 million events per day + 20 million network events per day.</p>	<p>11.5.1 Installation Up to 4 days with 28 days of historical data.</p> <p>11.5.1 Upgrade from 11.4.x No learning period.</p> <ul style="list-style-type: none"> • UEBA rerun is not required. <p>11.5.1 Upgrade from 11.3.x or prior versions Up to 4 days with 28 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <p>11.5.1 Upgrade with schema removal Up to 4 days with 28 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required
<p>Logs and Endpoint data for 100,000 users with 30 million events per day + 60 million network events per day.</p>	<p>11.5.1 Installation Up to 14 days with 14 days of historical data.</p> <p>11.5.1 Upgrade from 11.4.x No learning period.</p> <ul style="list-style-type: none"> • UEBA rerun is not required. <p>11.5.1 Upgrade from 11.3.x or prior versions Up to 14 days with 14 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p> <p>11.5.1 Upgrade with schema removal Up to 14 days with 14 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p>

Virtual Machine

If there is not historical data, then the learning period will be 28 days.

CPU	Memory	Read IOPS	Write IOPS
16 cores	64GB	500	500

Note: NetWitness recommends you to deploy UEBA on a virtual host, only if your log collection volume is low. If you have a moderate to high log collection volume, NetWitness recommends you to deploy UEBA on the physical host as described in the " NetWitness UEBA Host Hardware Specifications" topic of the *Physical Host Installation Guide*. Contact Customer Support (<https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897>) for advice on choosing which host, virtual or physical, to use for UEBA.

Supported Scale for existing NetWitness customers (historical data is available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for up to 100,000 users with 30 million events per day (no network data).	<p>11.5.1 Installation Up to 4 days with 28 days of historical data.</p> <p>11.5.1 Upgrade from 11.4.x No learning period.</p> <ul style="list-style-type: none"> • UEBA rerun is not required. <p>11.5.1 Upgrade from 11.3.x or prior versions Up to 4 days with 28 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <p>11.5.1 Upgrade with schema removal Up to 4 days with 28 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required

Supported Scale for existing NetWitness customers (historical data is available)	Learning Period Alerts will be generated when the learning period is complete
<p>Logs and Endpoint data for up to 100,000 users with 30 million events per day + 20 million network events per day.</p>	<p>11.5.1 Installation Up to 14 days with 14 days of historical data.</p> <p>11.5.1 Upgrade from 11.4.x No learning period.</p> <ul style="list-style-type: none"> • UEBA rerun is not required. <p>11.5.1 Upgrade from 11.3.x or prior versions Up to 14 days with 14 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <div data-bbox="800 793 1421 909" style="border: 1px solid green; padding: 5px;"> <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p> </div> <p>11.5.1 Upgrade with schema removal Up to 14 days with 14 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <div data-bbox="800 1087 1421 1203" style="border: 1px solid green; padding: 5px;"> <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p> </div>

Note: Network events per day refers to number of events consumed by UEBA per day. To determine the scale of network events for existing customers, see [Troubleshooting UEBA Configurations](#).

Learning Period Per Scale for 11.5

Physical Machine

SERIES 5 (DELL R630) SPECIFICATIONS

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for 100,000 users + 20 million network events per day.	Yes	11.5 Installation Up to 4 days with 28 days of historical data.
	Yes	11.5 Upgrade from 11.4.x with no schema changes No learning period. <ul style="list-style-type: none"> • UEBA rerun is not required.
	Yes	11.5 Upgrade from 11.3.x or prior versions with no schema changes Up to 4 days with 28 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required.
	Yes	11.5 Upgrade with schema changes Up to 4 days with 28 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
Logs and Endpoint data for 100,000 users + 60 million network events per day.	Yes	11.5 Installation Up to 14 days with 14 days of historical data.
	Yes	11.5 Upgrade from 11.4.x with no schema changes No learning period. <ul style="list-style-type: none"> • UEBA rerun is not required.
	Yes	11.5 Upgrade from 11.3.x or prior versions with no schema changes Up to 14 days with 14 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p> </div>
	Yes	11.5 Upgrade with schema changes Up to 14 days with 14 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p> </div>
Logs and Endpoint data for up to 100,000 users + 60 million network events per day.	No	11.5 Installation 28 days

Virtual Machine

CPU	Memory	Read IOPS	Write IOPS
16 cores	64GB	500	500

Note: NetWitness recommends you to deploy UEBA on a virtual host, only if your log collection volume is low. If you have a moderate to high log collection volume, NetWitness recommends you to deploy UEBA on the physical host as described in the "NetWitness UEBA Host Hardware Specifications" topic of the *Physical Host Installation Guide*. Contact Customer Support (<https://community.netwitness.com/t5/support-information/how-to-contact-netwitness-support/ta-p/563897>) for advice on choosing which host, virtual or physical, to use for UEBA.

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period <small>Alerts will be generated when the learning period is complete</small>
Logs and Endpoint data for up to 100,000 users with 30 million events per day (no network data).	Yes	11.5 Installation Up to 4 days with 28 days of historical data.
	Yes	11.5 Upgrade from 11.4.x with no schema changes No learning period. <ul style="list-style-type: none"> • UEBA rerun is not required.
	Yes	11.5 Upgrade from 11.3.x or prior versions with no schema changes Up to 4 days with 28 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required.
	Yes	11.5 Upgrade with schema changes Up to 4 days with 28 days of historical data. <ul style="list-style-type: none"> • UEBA rerun is required

Supported Scale	Existing NetWitness customer (historical data available)	Learning Period Alerts will be generated when the learning period is complete
<p>Logs and Endpoint data for up to 100,000 users with 30 million events per day + 20 million network events per day.</p>	Yes	<p>11.5 Installation Up to 14 days with 14 days of historical data.</p>
		<p>11.5 Upgrade from 11.4.x with no schema changes No learning period.</p> <ul style="list-style-type: none"> • UEBA rerun is not required.
		<p>11.5 Upgrade from 11.3.x or prior versions with no schema changes Up to 14 days with 14 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <div data-bbox="927 1087 1421 1236" style="border: 1px solid green; padding: 5px;"> <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p> </div>
		<p>11.5 Upgrade with schema changes Up to 14 days with 14 days of historical data.</p> <ul style="list-style-type: none"> • UEBA rerun is required. <div data-bbox="927 1444 1421 1593" style="border: 1px solid green; padding: 5px;"> <p>Note: This scenario is impacted by ASOC-101686 known issue. For more information, see <i>NetWitness Release Notes for 11.5</i>.</p> </div>
<p>Logs and Endpoint data for up to 100,000 users with 30 million events per day + 20 million network events per day.</p>	No	<p>11.5 Installation 28 days</p>

Note: Network events per day refers to number of events consumed by UEBA per day. To determine the scale of network events for existing customers, see [Troubleshooting UEBA Configurations](#).

Troubleshooting UEBA Configurations

This section provides information about possible issues when using NetWitness UEBA.

Task Failure Issues in Airflow

Problem	The <code>userId_output_entities</code> task fails when the username contains a backslash.
Cause	When events with usernames containing a backslash character is passed through UEBA, then the <code>userId_output_entities</code> task fails.
Solution	<p>To resolve this issue contact the customer success to obtain the relevant files and execute the following steps:</p> <ul style="list-style-type: none"> • Stop <code>airflow-scheduler</code> service. • Remove all MongoDB documents in the "aggr", "accm" and "input" collections that contains <code>context.userId</code> with hashtag. These documents can be located using the <code>FindCollecionsContainsBackslash.js</code> script. • Replace the <code>/var/netwitness/presidio/asl/adapters-config/transformers/adapters/authentication.json</code> file with the updated <code>authentication.json</code>. • Restart the <code>airflow-scheduler</code> service. • Validate that the next run of the <code>userId_output_entities</code> task is completed successfully.

Problem	The <code>AUTHENTICATION_userId_build_feature_historical_data</code> task fails when the username contains a hashtag.
Cause	When events with usernames containing a hashtag character is passed through UEBA, then the <code>AUTHENTICATION_userId_build_feature_historical_data</code> task fails.
Solution	<p>To resolve these issue contact the customer success to obtain the relevant files and execute the following steps:</p> <ul style="list-style-type: none"> • Stop <code>airflow-scheduler</code> service. • Remove all MongoDB documents in the "aggr", "accm" and "input" collections that contains <code>context.userId</code> with hashtag. These documents can be located using the <code>FindCollecionsContainsHashtagContextUserId.js</code> script.

	<ul style="list-style-type: none"> • Replace the <code>/var/netwitness/presidio/asl/adapter-config/transformers/adapter/authentication.json</code> file with the updated authentication .json. • Restart the <code>airflow-scheduler</code> service. • Validate that the next run of <code>AUTHENTICATION_userId_build_feature_historical_data</code> task is completed successfully.
--	--

Problem	The task <code>output_forwarding_task</code> fails in Airflow UI for <code>userId_hourly_ueba_flow</code> DAG due to Elasticsearch 'too many clauses' exception.
Cause	The <code>output_forwarding_task</code> task in the <code>userId_hourly_ueba_flow</code> DAG fails in the Airflow UI. The failure is caused by an Elasticsearch exception with the following message: <code>"caused_by":{"type":"too_many_clauses","reason":"maxClauseCount is set to 1024"}</code> . The <code>too_many_clauses</code> error occurs when the number of clauses in an Elasticsearch query exceeds the maximum limit set by the system. In this case, the maximum number of clauses was set to 1024. The <code>output_forwarding_task</code> exceeded this limit, which caused the failure.
Solution	<p>To increase the max clause count value, execute the following steps:</p> <ol style="list-style-type: none"> 1. SSH to UEBA server. 2. Open the <code>/etc/elasticsearch/elasticsearch.yml</code> file. 3. Update the max clause count parameter value: <pre>indices.query.bool.max_clause_count: 1500</pre> 4. Restart the elasticsearch service using the following command: <pre>systemctl restart elasticsearch</pre> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: After restarting, the task may fail and will be automatically retried.</p> </div>

Problem	Task failure in root DAG due to Airflow issue.
Cause	In the root DAG, one of the tasks failed unexpectedly due to an existing issue with the airflow system.

Solution


Whenever this issue occurs, you must examine the logs related to the specific failed task and verify whether the following log entry is present: `dagrun.py:465} INFO - (psycpg2.errors.UniqueViolation) duplicate key value violates unique constraint "task_instance_pkey"`. In such situations, you can safely ignore this issue as it does not require further action.

Note: This issue does not impact the functionality of UEBA.

MongoDB I/O Operations Slowness Issue

Problem	Increased execution time for DAGs with Mongo I/O Operations.
Cause	Some of the DAGs in the system experienced increased execution time due to slow MongoDB Input/Output (I/O) operations.
Solution	<p>To increase the MongoDB cache size in the MongoDB config file, execute the following steps:</p> <ol style="list-style-type: none"> 1. SSH to UEBA server. 2. Open the <code>/etc/mongod.conf</code> file. 3. Update the <code>internalQueryMaxBlockingSortMemoryUsageBytes</code> value to 1GB (1053554432 bytes). <pre>internalQueryMaxBlockingSortMemoryUsageBytes: 1053554432</pre> 4. Restart the Mongod service using the following command: <pre>systemctl restart mongod</pre> <p>Note: After restarting, the task may fail and will be automatically retried.</p>

User Interface Inaccessible

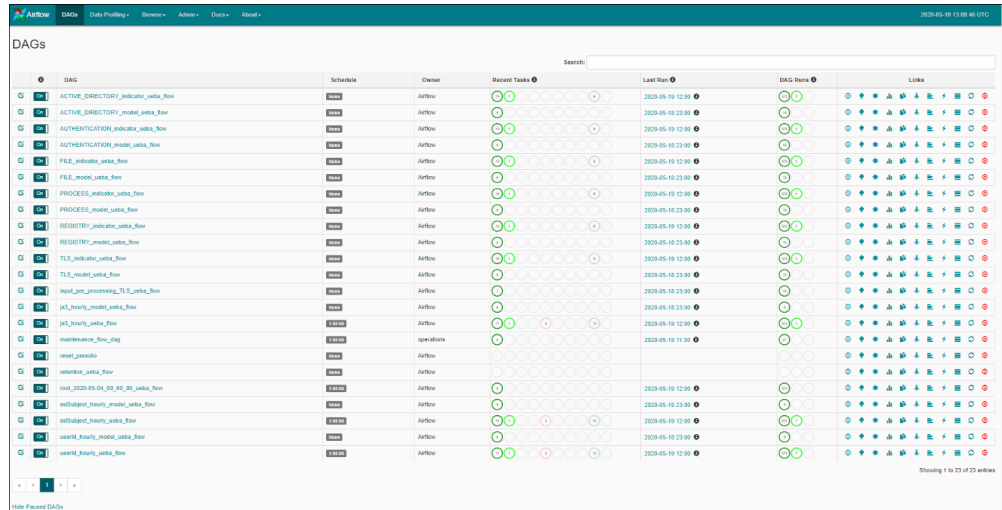
Problem	The User Interface is not accessible.
Cause	You have more than one NetWitness UEBA service existing in your NetWitness deployment and you can only have NetWitness UEBA service in your deployment.
Solution	<p>Complete the following steps to remove the extra NetWitness UEBA service.</p> <ol style="list-style-type: none"> 1. SSH to NW Server and run the following commands to query the list of installed NetWitness UEBA services. <pre># orchestration-cli-client --list-services grep presidio-airflow ... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true ... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true</pre> 2. From the list of services, determine which instance of the presidio-airflow service should be removed (by looking at the host addresses). 3. Run the following command to remove the extra service from Orchestration (use the matching service ID from the list of services): <pre># orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output></pre> <div style="border: 1px solid green; padding: 5px; margin: 10px 0;"> <p>Note: Run the following command to update NW Server to restore NGINX:</p> <pre># orchestration-cli-client --update-admin-node</pre> </div> 4. Log in to NetWitness, go to  (Admin) > Hosts, and remove the extra NetWitness UEBA host.

Get UEBA Configuration Parameters

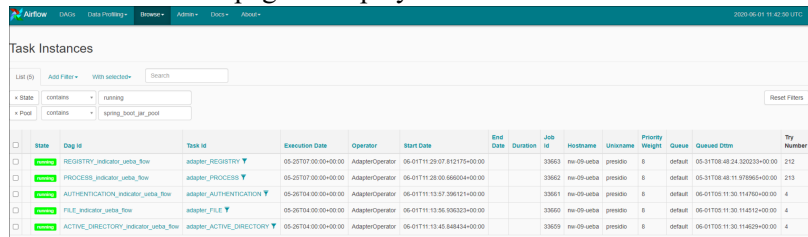
Issue	How to get UEBA configuration parameters?
Explanation	To get the UEBA configuration main parameters, run the <code>curl http://localhost:8888/application-default.properties</code> command from the UEBA host.

Resolution

1. Navigate to <https://<UEBA-host-name>/admin>. Enter the admin username and the deploy-admin password. The following image is of the Airflow home page that shows the system is working as expected.



2. Make sure that no red or yellow circles appear in the main page:
 - red circle indicates that a task has failed.
 - yellow circle indicates that a task has failed and is “awaiting” for a retry. If a “failed” or “up-for-retry” task appears, investigate what is the root cause of the problem.
3. Make sure the system continues to run.
4. Tap the **Browse** button and select **Task Instance**.
5. Add the following filters: **State** = running and **Pool** = spring_boot_jar_pool. The Task Instance page is displayed.



The **Execution Date** column shows the current time window for each running task. Make sure the execution date is greater than the UEBA start-date and that new tasks have an updated date are added to the table.

Check if data is received on the UEBA by Kibana

Issue

How to check if data is received on the UEBA by Kibana

Explanation

Navigate to <https://<UEBA-host-name>/kibana>. Enter the admin username and the deploy-admin password: To check that the data is flowing to the UEBA go to the Adapter Dashboard: Tap the Dashboard tab in the left menu Tap Adapter Dashboard at the right menu Select the relevant time range at the top bar The charts on this dashboard will present you the data that already fetched by the UEBA.

Scaling Limitation Issue

When installed on a Virtual Machine, you can determine the number of network events to be processed by referring to the latest version of the **Learning Period Per Scale** topic.

Note: If the scaling limits are exceeded, NetWitness recommends provisioning the UEBA on a physical appliance.

Issue	How to determine the scale of network events currently available, to know if it exceeds the UEBA limitation.
Solution	<p>To know the network data limit, perform the following :</p> <ul style="list-style-type: none"> • Run the query on the Broker or Concentrator that connects to UEBA using NetWitness UI: <pre>service=443 && direction='outbound' && analysis.service!='quic' && ip.src exists && ip.dst exists && tcp.srcport!=443</pre> <p>Calculate the total number of events for the selected days (including weekdays with standard workload). To determine the number of network events to be processed on a virtual machine for your environment, always refer to the latest version of the Learning Period for Scale topic.</p>

Issue	Can UEBA for Packets be used if UEBA's supported scale is exceeded?
Solution	<p>You must create or choose a Broker that is connected to a subset of Concentrators that does not exceed the supported limit.</p> <p>To know the network data limit, perform the following :</p> <ul style="list-style-type: none"> • Run the query on the Concentrator that connects to UEBA using NetWitness UI:

	<pre>service=443 && direction='outbound' && analysis.service!='quic' && ip.src exists && ip.dst exists && tcp.srcport!=443</pre> <p>Calculate the total number of events for the selected days (including weekdays with standard workload). If the average is above 20 million per day then it indicates that UEBA's supported scale is exceeded.</p>
--	---

Note: The Broker must query all the available and needed data needed such as logs, endpoint and network (packets). UEBA packets models are based on the whole environment. Hence, make sure that the data parsed from the subset of Concentrators is consistent.

UEBA Policy Issue

Issue	<p>After you create a rule under UEBA policy, duplicate values are displayed in the Statistics drop-down.</p>
Solution	<p>To remove the duplicate values, perform the following:</p> <ol style="list-style-type: none"> 1. Log in to MongoDB using following command: <pre>mongo admin -u deploy_admin -p {Enter the password}</pre> 2. Run the following command on MongoDB: <pre>use sms; db.getCollection('sms_statdefinition').find({componentId :"presidioairflow"}) db.getCollection('sms_statdefinition').deleteMany ({componentId : "presidioairflow"})</pre>

Troubleshoot Using Kibana

Issue	<p>After you deploy NetWitness UEBA, the connection between the NetWitness and NetWitness UEBA is successful but there are very few or no events in the Users > OVERVIEW tab.</p> <ol style="list-style-type: none"> 1. Log in to Kibana. 2. Go to Table of Content > Dashboards > Adapter Dashboard. 3. Adjust the Time Range on the top-right corner of the page and review the following: <ul style="list-style-type: none"> • If the new events are flowing. • In the Saved Events Per Schema graph, see the number of successful events per schema per hour. • In the Total Events vs. Success Events graph, see the total number of events and number of successful events. The number of successful events should be more every hour. <p>For example, in an environment with 1000 users or more, there should be thousands</p>
-------	---

	of authentication and file access events and more than 10 Active Directory events. If there are very few events, there is likely an issue with Windows auditing.
Solution	<p>You must identify the missing events and reconfigure the Windows auditing.</p> <ol style="list-style-type: none"> 1. Go to Investigate > Navigate. 2. Filter by device.type= device.type “winevent_snare” or “winevent_nic”. 3. Review the events using reference.id meta key to identify the missing events. 4. Reconfigure the Windows auditing. For more information, see NetWitness UEBA Windows Audit Policy topic.

Issue	The historical load is complete and the events are coming from Adapter dashboard but no alerts are displayed in the Users > Overview tab.
Solution	<ol style="list-style-type: none"> 1. Go to Kibana > Table of content > Scoring and model cache. 2. Adjust the Time Range from the top-right corner of the page, and see if the events are scored.

Issue	The historical load is complete but no alerts are displayed in the Users tab.
Solution	<ol style="list-style-type: none"> 1. Go to Kibana > Dashboard > Overview. 2. Adjust the Time Range from the top-right corner of the page, and see how many users are analyzed and if any anomalies are found.

Troubleshoot Using Airflow

Issue	After you start running the UEBA it is not possible to remove a data source during the run process else the process stops.
Solution	You must either continue the process till it completes or remove the required data source from UEBA and rerun the process.

Issue	After you deploy UEBA and if there are no events displayed in the Kibana > Table of content > Adapter dashboard and Airflow has already processed the hours but there are no events. This is due to some communication issue.
Solution	<p>You must check the logs and resolve the issue.</p> <ol style="list-style-type: none"> 1. Log in to Airflow. 2. Go to Admin > REST API Plugin. 3. In the Failed Tasks Logs, click execute.

A zip file is downloaded.

4. Unzip the file and open the log file to view and resolve the error.
5. In the **DAGs > reset_presidio**, click **Trigger Dag**.
This deletes all the data and compute all the alert from the beginning.

Note: During initial installation, if the hours are processed successfully but there are no events, you must click reset_presidio after fixing the data in the Broker. Do not reset if there are alerts.