NetWitness® Platform

Version 12.4

UEBA Standalone Installation Guide

NETWITNESS

Platform

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 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/.

April, 2024

Contents

Introduction

NetWitness® UEBA standalone installation is designed to support other security tools such as Security Information and Event Management (SIEM). It allows users of a third-party SIEM solutions to leverage NetWitness for UEBA.

NetWitness® UEBA standalone installation includes:

1. NetWitness Admin Server

2. NetWitness Log Hybrid

3. NetWitness UEBA

> **Note:** NetWitness® UEBA standalone installation supports up to 100,000 users on a single running instance. If you have more than 100,000 users, contact Customer Support.

Windows Log Sources

NetWitness UEBA standalone installation natively supports the following Windows log sources:

- Windows Active Directory
- Windows Logon and Authentication Activity
- Windows File Servers
- Windows Remote Management

For more information, see the "NetWitness UEBA Use Cases for Windows Logs" topic in the *NetWitness UEBA User Guide*.

NetWitness UEBA Standalone Installation

This section contains a high-level UEBA standalone installation diagram and a list of NetWitness UEBA ports.

The following diagram illustrates the NetWitness UEBA standalone installation.
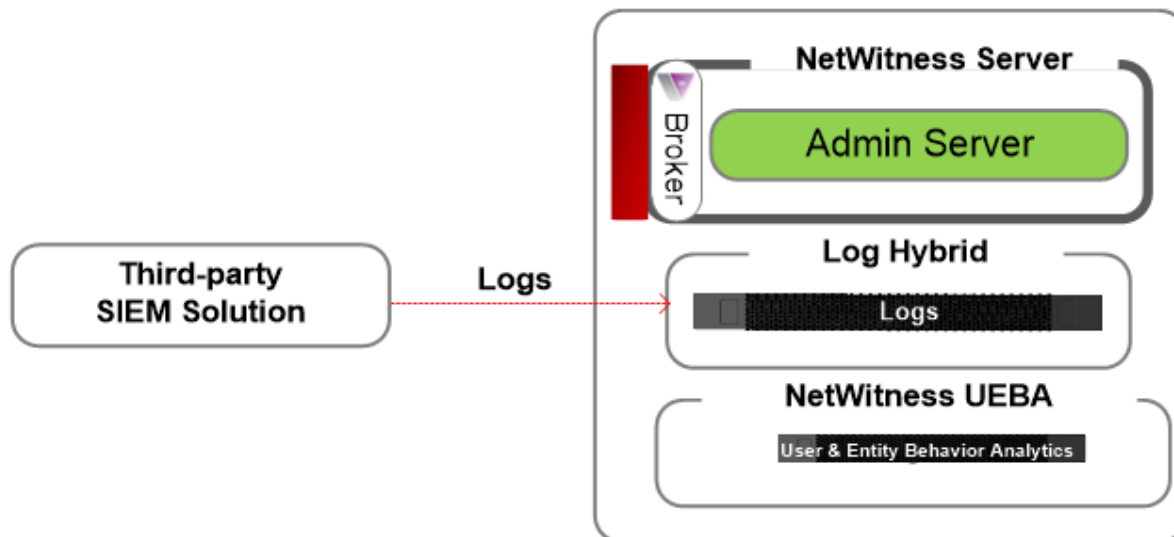
Note:
- UEBA connects to the Broker or Log Hybrid host.
- To configure the Log Hybrid for logs from a third-party SIEM, contact your RSA Account Manager.

UEBA Host and Service Ports

Source Host	Destination Host	Destination Ports	Comments
UEBA Server	NW Server	TCP 443	NetWitness Update Repository
UEBA Server	NW Server	TCP 56003 (SSL), 50003 (Non-SSL), 50103 (REST)	Broker Application Ports
UEBA Server	NW Server	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Log Hybrid, Concentrator Application Ports
Admin Workstation	UEBA Server	443	UEBA Monitoring
Admin Workstation	UEBA Server	22	SSH
Admin Workstation	UEBA Server	8100	Airflow UI

System Requirements

You can run the NetWitness® UEBA standalone installation as follows:

- NetWitness Physical Hosts (software running on hardware supplied by NetWitness)
  - Install physical hosts and connect to the network as described in the NetWitness® Platform Hardware Setup Guides and the *NetWitness® Platform Physical Host Installation Guide 12.4 version*.
  - Set up licensing for NetWitness Platform as described in the *NetWitness® Platform Licensing Guide*.
- On-Premises (On-Prem) Virtual Hosts (Software Only provided by Netwitness)

Physical Host Hardware Specifications

You must install the NetWitness UEBA host on the S6 (Dell R640 appliance) hardware.

SERIES 6 SPECIFICATIONS

Item	Core	ESA/Analytics	Hybrid
Host Type	NW Server, Log Decoder, Network Decoder (Packets), Concentrator, Broker, Archiver, Malware Analysis	ESA UEBA	Log Decoder Hybrid, Network Decoder Hybrid (Packets), Endpoint Log Hybrid
Model	Dell PowerEdge R640	Dell PowerEdge R640	Dell PowerEdge R740
Processor			
Type	Intel Xeon Gold 6134	Intel Xeon Gold 6126	Intel Xeon Gold 6132
Processor Speed	3.2Ghz	2.6Ghz	2.6Ghz
Cache	24.75M 1 Cache	19.25M Cache	19M Cache
# of Processors	2	2	2
# of Cores	8 Cores per Processor	12 Cores per Processor	14 Cores per Processor
# of Threads	16 Threads per Processor	24 Threads per Processor	28 Threads per Processor

Item	Core	ESA/Analytics	Hybrid
Series 6 Hard Drives Field replaceable Hot swappable	2 X 1TB NL-SAS 7.2K 2 X 2TB NL-SAS 7.2K Total - 4 Drives Slots 0-1: 1TB Slots 2-3: 2TB	2 X 1TB NL-SAS 7.2K 4 X 2.4TB SAS 10K Total - 6 Drives Slots 0-1: 1TB Slots 2-5: 2.4TB	4 X 2TB NL-SAS 7.2K 8 X 8TB NL-SAS 7.2K 2 x 1.6TB SSD Total - 14 Drives Slots 0-3 (Front): 2TB Slots 4-11 (Front): 8TB Slots 12-13 (Rear): 1.6TB SSD
Series 6E Self-Encrypting Drives (SEDs) FIPS140 Certified Field replaceable Hot swappable	2 X 1.2TB SAS 10K SED 2 X 2.4TB SAS 10K SED Total - 4 Drives Slots 0-1: 1.2TB Slots 2-3: 2.4TB	2 X 1.2TB SAS 10K SED 4 X 2.4TB SAS 10K SED Total - 6 Drives Slots 0-1: 1.2TB Slots 2-5: 2.4TB	2 X 2.4TB SAS 10K SED 10 X 8TB NL-SAS 7.2K SED 2 x 1.92TB SSD SED Total - 14 Drives Slots 0-1 (Front): 2.4TB Slots 2-11 (Front): 8TB Slots 12-13 (Rear): 1.92TB SSD
Memory	128GB 4 * 32GB RDIMM 2666MT/s Dual Rank	256GB 8 * 32GB RDIMM 2133MT/s	128GB 4 * 32GB RDIMM 2666MT/s Dual Rank
Storage Controllers	External PERC H840, Internal PERC H740P		
Network Interface Card	Intel X710 DP 10Gb DA/SFP+, + 1350 DP 1Gb Ethernet, Network Daughter Card		
Power			
PSU	Dual, Hot-plug, Redundant Power Supply (1+1), 1100 W AC		
BTU/hr	4100 BTU/hr (Maximum)		
Voltage	100-240 V AC, autoaranging		
Current	12 A - 6.5 A		
Form Factor	1U, full depth		2U, full depth
Weight (approximate)	21.9 kg (48.28 lbs)		33.1 kg (72.91 lb)
Dimensions (approximate)	With bezel: 482.0 mm (18.97 in) [w] x 808.51 mm (31.83 in) [d] x 42.8 mm (1.68 in) [h] Without bezel: 482.0 mm (18.97 in) [w] x 794.67 mm (31.29 in) [d] x 42.8 mm (1.68 in) [h]		With bezel: 482.0 mm (18.98 in) [w] x 751.34 mm (29.58 in) [d] x 86.8 mm (3.42 in) [h] Without bezel: 482.0 mm (18.98 in) [w] x 737.50 mm (29.04 in) [d] x 86.8 mm (3.42 in) [h]

Item	Core	ESA/Analytics	Hybrid
Shipping Dimensions	Server boxed for shipping (includes rail kit) Height: 30.48 cm (12 inch) Width: 104.14 cm (41 inch) Depth: 64.14 cm (25.25 inch) Weight: 25.85 kg (57 lb)		Server boxed for shipping (includes rail kit) Height: 32.39 cm (12.75 inch) Width: 95.25 cm (37.50 inch) Depth: 66.04 cm (26.00 inch) Weight: 35 kg (81.86 lb)
Throughput / EPS	Network: 2-10 Gbps Logs: 30K EPS	N/A	Network: 1 Gbps Logs: 20K EPS
Supported SFPs & Add-On Cards	Add-On Cards 1G QP Intel Copper Adapter 10G DP Intel Copper Adapter 10G DP Intel Optical Adapter External PERC H840 16G DP Emulex HBA SFPs 1G SFP Intel Copper 10G SFP Short Range Intel Optical (standard) 10G SFP Long Range Intel Optical		

* NIC Card options are available for swap with on-board daughter card or add on.

Virtual Host Specifications

Following is the recommended system requirements for a UEBA virtual host.

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	• Storage: 1.5 TB • Provisioning: Thick	500	500

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-provisoned disk for storage usage.

Note: NetWitness recommends that you only deploy UEBA on a virtual host if your log collection volume is low. If you have a moderate to high log collection volume, NetWitness recommends that you deploy UEBA on the physical host.

Installation Media

Installation media are in the form of OVA packages, which are available for download and installation from Download Central. As part of your order fulfillment, NetWitness gives you access to the OVA.

Installation Tasks

This topic contains the tasks you must complete to install NetWitness UEBA standalone installation.

> **Note:** Download or make sure you have access to the *Physical Host Installation Guide* for Version 12.4 before beginning the tasks. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

For Physical Hosts:

You need to complete the following tasks in the order shown below.

Task 1. Install 12.4 on the NetWitness Server Host

Task 2. Install 12.4 Log Hybrid Host

Task 3. Install and Configure NetWitness® UEBA

Task 1. Install 12.4 on the NetWitness Server Host

For the NetWitness Server (NW Server), this task:

- Creates a base image.

- Sets up the 12.4 NW Server host.

For more information on how to install the NetWitness Server host, see "Install 12.4 on the NetWitness Server (NW Server) Host" section in the *Physical Host Installation Guide for Version 12.4*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Task 2. Install 12.4 Log Hybrid Host

For a non-NW Server host, this task:

- Creates a base image.

- Sets up the 12.4 non-NW Server host or Log Hybrid.

For more information on how to install the Log Hybrid host, see "Task 2 - Install 12.4 on Other Component Hosts" section in the *Physical Host Installation Guide for Version 12.4*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Task 3. Install and Configure NetWitness® UEBA

To set up NetWitness UEBA, you must install and configure the NetWitness UEBA service.

The following procedure shows you how to install the NetWitness UEBA service on a NetWitness UEBA Host Type and configure the service.

1. Complete steps 1 - 14 under "Task 2 - Install 12.4 on Other Component Hosts" in "Installation Tasks" of the *NetWitness Platform Physical Host Installation Guide for Version 12.4*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

   Note: The Kibana and Airflow webserver User Interface password is the same as the deploy_ admin password. Make sure that you record this password and store it in a safe location.

2. Log in to the NetWitness Platform and go to ✂ **(Admin) > Hosts**.

   The New Hosts dialog is displayed with the Hosts view grayed out in the background.

   Note: If the New Hosts dialog is not displayed, click **Discover** in the **Hosts** view toolbar.

3. Select the host in the **New Hosts** dialog and click **Enable**.

   The New Hosts dialog closes and the host is displayed in the Hosts view.

4. Select that host in the **Hosts** view (for example, **UEBA**) and click 🔧 Install ⊙.

   The Install Services dialog is displayed.

5. Select the **UEBA** Host Type and click **Install**.
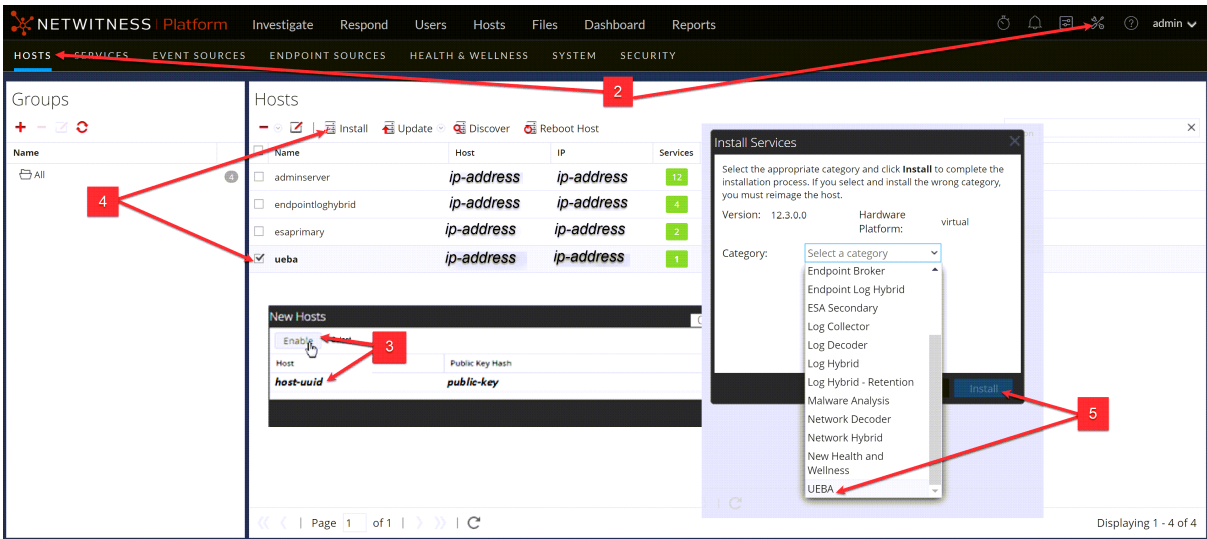
6. Make sure that the UEBA service is running.

7. Complete licensing requirements for NetWitness UEBA.

   See the *NetWitness Platform 12.4 Licensing Management Guide* for more information. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

   Note: NetWitness Platform supports the User and Entity Behavior Analytics License (UEBA). This license is used based on the number of users. The Out-of-the-Box Trial License is a 90-day trial license. In case of UEBA licenses, the 90-day trial period begins from the time the UEBA service deployed on the NetWitness Platform product.

Configure NetWitness UEBA

To start running UEBA:

1. Define the following parameters: data schemas, data source (NetWitness Broker or Concentrator) and start date.

    a. Define UEBA schemas:
    Choose schemas from the following list:

    AUTHENTICATION, FILE, ACTIVE_DIRECTORY, PROCESS, REGISTRY and TLS.

    > **Note:** The TLS packet requires adding the hunting package and enabling the JA3 feature. For more information regarding events that each schema contains, see the *NetWitness UEBA Configuration Guide*.

    b. Define the data source:
    If your deployment has multiple Concentrators, we recommend that you assign a Broker at the top of your deployment hierarchy for the NetWitness UEBA data source.

    c. Define the UEBA start-date:

    > **Note:** The selected start date must contain events from all configured schemas.

    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 make sure that the start date is set to no later than 14 days earlier than the current date.

2. . Create a user account for the data source (Broker or Concentrator) to authenticate to the data.

    a. Log in to the NetWitness Platform.

    b. Go to ✂ (Admin) > **Services**.

    c. Locate the data source service (Broker or Concentrator).
    Select that service, and select ⚙ ⌄ **(Actions)** > **View** > **Security**.

    d. Create a new user and assign the "Analysts" role to that user.

The following example shows a user account created for a Broker.
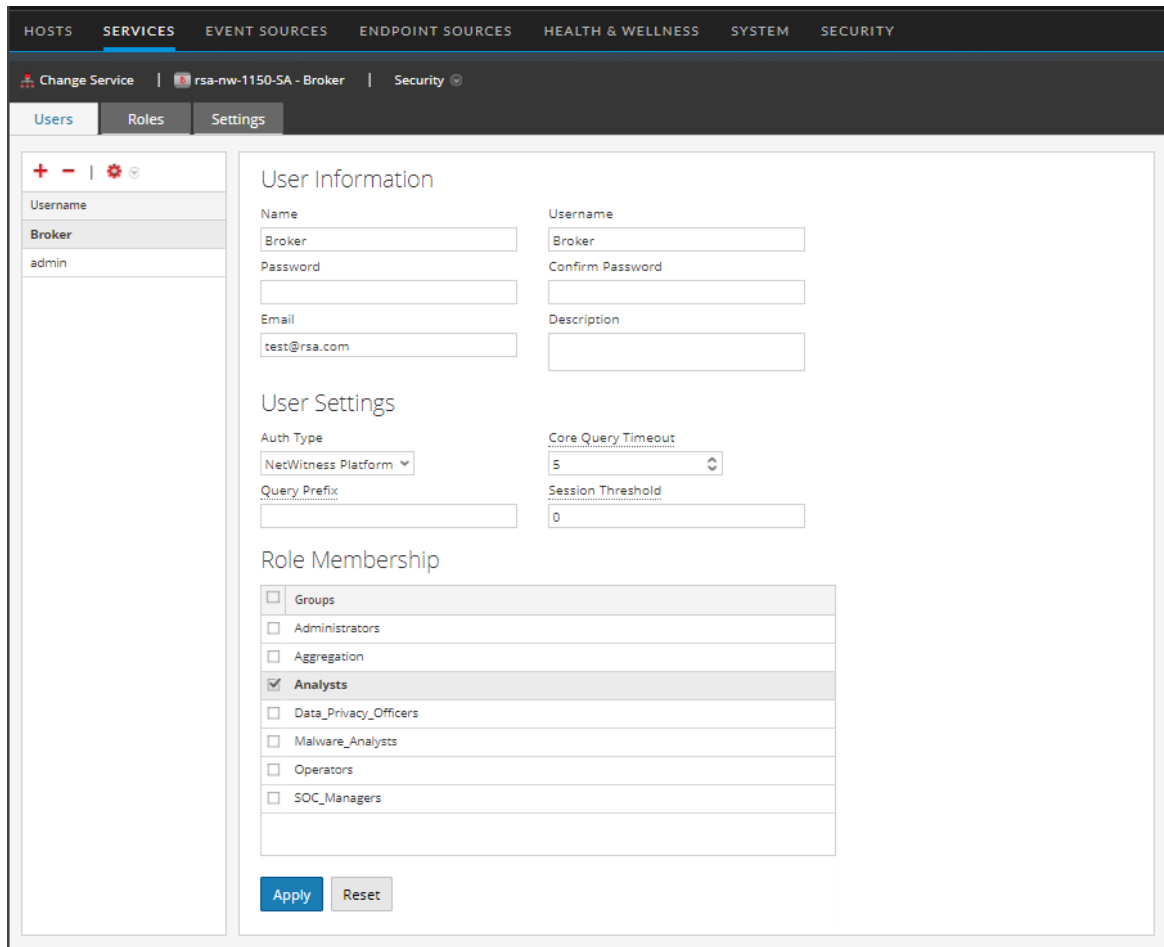
3. SSH to the NetWitness UEBA server host.

4. (For Virtual Machines Only) Set the appropriate parallelism value:
If the UEBA system runs on VM, update the airflow parallelism value to be 64 by running the following command:
```
sed -i "s|parallelism = 256|parallelism = 64|g"
/var/netwitness/presidio/airflow/airflow.cfg
```

5. Submit the following commands with the above parameters that you already defined.
```
/opt/rsa/saTools/bin/ueba-server-config -u <user> -p <password> -h <host> -
o <type> -t <startTime> -s <schemas> -v -e <argument>
```
Where:

Argument	Variable	Description
-u	<user>	User name of the credentials for the Broker or Concentrator instance that you are using as a data source.

Argument	Variable	Description
-p	`<password>`	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. `!"#$%&()*+,-:;<=>?@[\]^_`\{|}`  If you want to include a special character or special characters, you must delimit the password with an apostrophe sign, for example: `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`
-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`).
-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 Installation Tasks.

6. Set the appropriate "Boot Jar Pools" slots:

- **Physical Appliance**: Update the `spring_boot_jar_pool`" slots to be 18.

- **Virtual Appliance**: If the UEBA system is running on VM, update the `spring_boot_jar_pool` and the `retention_spring_boot_jar_pool` slots values to 5.
  To update the "Spring Boot Jar Pools" slots, Go to the Airflow main page, tap the "Admin" tab at the top bar and tap "Pools".

a. To access the Airflow UI, go to `https://<UEBA_host>/admin` and enter the credentials.

• User: admin

• Password: The environment deploy admin password.

b. Click on the pencil mark of the polls to update the slot values.

Enable Access Permission for the NetWitness UEBA User Interface

After you install NetWitness UEBA standalone 12.4, you need to assign the UEBA_Analysts and Analysts roles to the UEBA users. For more information, see 'Assign User Access to UEBA' topic in the *NetWitness UEBA Configuration Guide*. After this configuration, UEBA users can access the **Investigate** > **Users** view.

> **Note:** To complete NetWitness UEBA configuration according to the needs of your organization, See the *NetWitness UEBA Configuration Guide*.

For Virtual Hosts

You must complete the following tasks in the order shown below.

Task 1. Install 12.4 on the NetWitness Server Host

Task 2. Install 12.4 Log Hybrid Host

Task 3. Install and Configure NetWitness® UEBA

Task 1. Install 12.4 on the NetWitness Server Host

On the host you have deployed for the NetWitness Server (NW Server), this task installs:

- The 12.4 NW Server environmental platform.

- The NW Admin Server.

- A repository with the RPM files required to install the other functional components or services.

For more information on how to install the NetWitness Server host, see "Task 1- Install 12.4 on the NW Server Host" section in the *Virtual Host Installation Guide for Version 12.4*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Task 2. Install 12.4 Log Hybrid Host

Complete the following tasks on a non-NW Server host:

- Install the 12.4 environmental platform.

- Apply the 12.4 RPM files to the service from the NW Server Update Repository.

> **Note:** You must install the Log Hybrid host.

For more information on how to install the non-NetWitness Server host, see "Task 3 - Install 12.4for on Other Component Hosts" section in the *Virtual Host Installation Guide for Version 12.4*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues..

Task 3. Install and Configure NetWitness® UEBA

Prerequisite: Increase Memory for Virtual Deployment

Virtual Machines are deployed with approximately 104 GB in the storage mount by default. To install NetWitness UEBA, you must increase the storage space in your virtual environment to at least 800 GB.

To set up NetWitness UEBA, you must install and configure the NetWitness UEBA service.

The following procedure shows you how to install the NetWitness UEBA service on a NetWitness UEBA Host Type and configure the service.

1. Complete steps 1 - 15 for Virtual Hosts under "Task 3 - Install 12.4 on Other Component Hosts" in "Installation Tasks" of the *NetWitness Platform Virtual Host Installation Guide for Version 12.4*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

> **Note:** The Kibana and Airflow webserver User Interface password is the same as the deploy admin password. Make sure that you record this password and store it in a safe location.

2. Complete steps 2 - 9 under Task 3. Install and Configure NetWitness® UEBA.

Post Installation Task

Set a user with privileges to access the UEBA Pages

After you install NetWitness UEBA standalone 12.4, you need to assign the **UEBA_Analysts** and **Analysts** roles to the UEBA users. For more information, see *NetWitness UEBA Configuration Guide*.