



UEBA Standalone Installation Guide

for RSA NetWitness® Platform 11.3



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

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

Trademarks

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

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

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

May 2019

Contents

Introduction	4
Windows Log Sources	4
RSA NetWitness UEBA Standalone Installation	5
UEBA Host and Service Ports	5
System Requirements	6
Physical Host Hardware Specifications	6
Virtual Host Specifications	7
Installation Media	7
Installation Tasks	8
For Physical Hosts:	8
Task 1. Install 11.3 on the NetWitness Server Host	8
Task 2. Install 11.3 Log Hybrid Host	8
Task 3. Install and Configure RSA NetWitness® UEBA	8
For Virtual Hosts:	13
Task 1. Install 11.3 on the NetWitness Server Host	13
Task 2. Install 11.3 Log Hybrid Host	15
Task 3. Install and Configure RSA NetWitness® UEBA	15
Post Installation Task	16
Set up Permission	16
Appendix: NetWitness UEBA Standalone Installation Windows Audit Policy	17
Troubleshooting	18
Install Only One Instance of the NetWitness UEBA Server	18
Contact Customer Support	18

Introduction

RSA 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 RSA NetWitness for UEBA.

RSA NetWitness® UEBA standalone installation includes:

1. NetWitness Admin Server
2. NetWitness Log Hybrid
3. NetWitness UEBA

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

Windows Log Sources

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

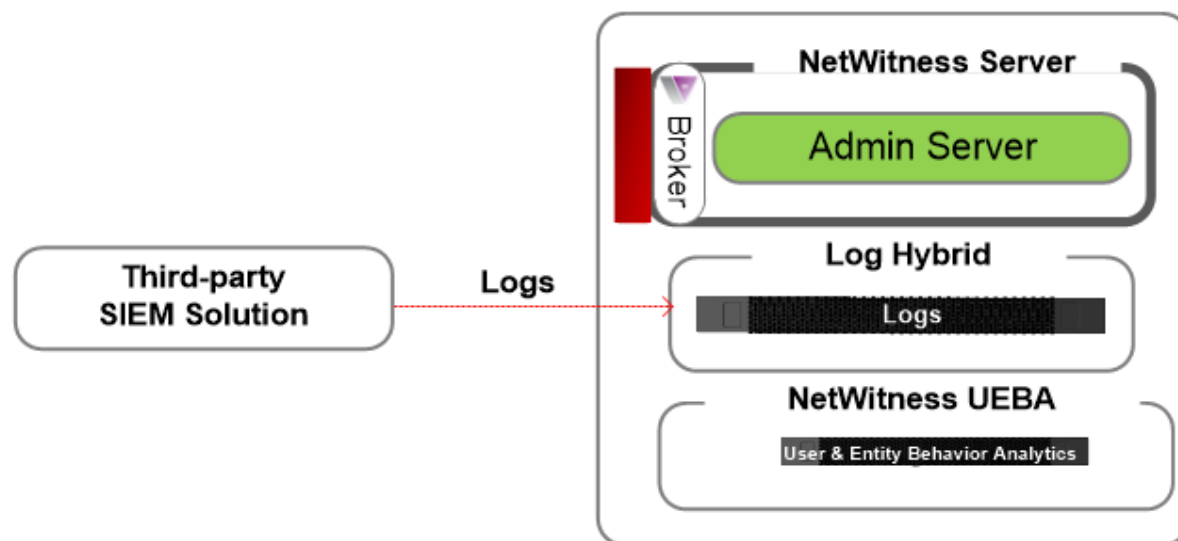
- Windows Active Directory
- Windows Logon and Authentication Activity
- Windows File Servers

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

RSA 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	RSA 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

System Requirements

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

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

Physical Host Hardware Specifications

You must install the NetWitness UEBA host on the S5 (Dell R630) or S6 (Dell R640) hardware.

SERIES 5 (DELL R630) SPECIFICATIONS

Specification	Capacity
Model	Dell PowerEdge R630xl
Processor Type	Intel Xeon E5 -2680v3
Processor Speed	2.5 GHz
Cache	30MB
Number of Cores	12
Number of Processors	2
Number of Threads	24
Total Memory	256GB
Internal Disk Controller	Dell PERC H730
External Disk Controller	Dell PERC H830
SAN Connectivity (HBA) - Optional	N/A
Remote Management Card	iDRAC8 Enterprise
Drives	<u>Total - 6 Drives</u> 2 x 1TB, 2.5" HDD 4 x 2TB, 2.5" HDD
Chassis	1U
Weight	18.4 kg (40.5 lbs)

Specification	Capacity
NIC Card*	<u>On Board</u> 2 x 10 Gb Copper 2 x 10 Gb & 2 x 1Gb Copper (Other options are available)
Dimensions	H: 4.28 cm (1.68 in.) x W: 48.23 cm (18.98 in.) x D: 75.51 cm (29.72 in.)
Power	1100W Redundant
BTU/hr	4100 BTU/hr (max)
Amps (Spec)	1100W / 220VAC = 5A
Actual Amp Draw (Post Startup)	2.1 Amps
Events Per Second (EPS)	100K EPS
Throughput	N/A

* 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.

CPU	Memory	Read IOPS	Write IOPS
16 or 2.4GHz	64 GB	500	500

Note: RSA 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, RSA 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 (<https://download.rsasecurity.com>). As part of your order fulfillment, RSA 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 11.3 before beginning the tasks. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

For Physical Hosts:

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

[Task 1. Install 11.3 on the NetWitness Server Host](#)

[Task 2. Install 11.3 Log Hybrid Host](#)

[Task 3. Install and Configure RSA NetWitness® UEBA](#)

Task 1. Install 11.3 on the NetWitness Server Host

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

- Creates a base image.
- Sets up the 11.3 NW Server host.

For more information on how to install the NetWitness Server host, see "Install 11.3 on the NetWitness Server (NW Server) Host" section in the *Physical Host Installation Guide for Version 11.3*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

Task 2. Install 11.3 Log Hybrid Host

For a non-NW Server host, this task:

- Creates a base image.
- Sets up the 11.3 non-NW Server host or Log Hybrid.

For more information on how to install the Log Hybrid host, see "Task 2 - Install 11.3 on Other Component Hosts" section in the *Physical Host Installation Guide for Version 11.3*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

Task 3. Install and Configure RSA 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.

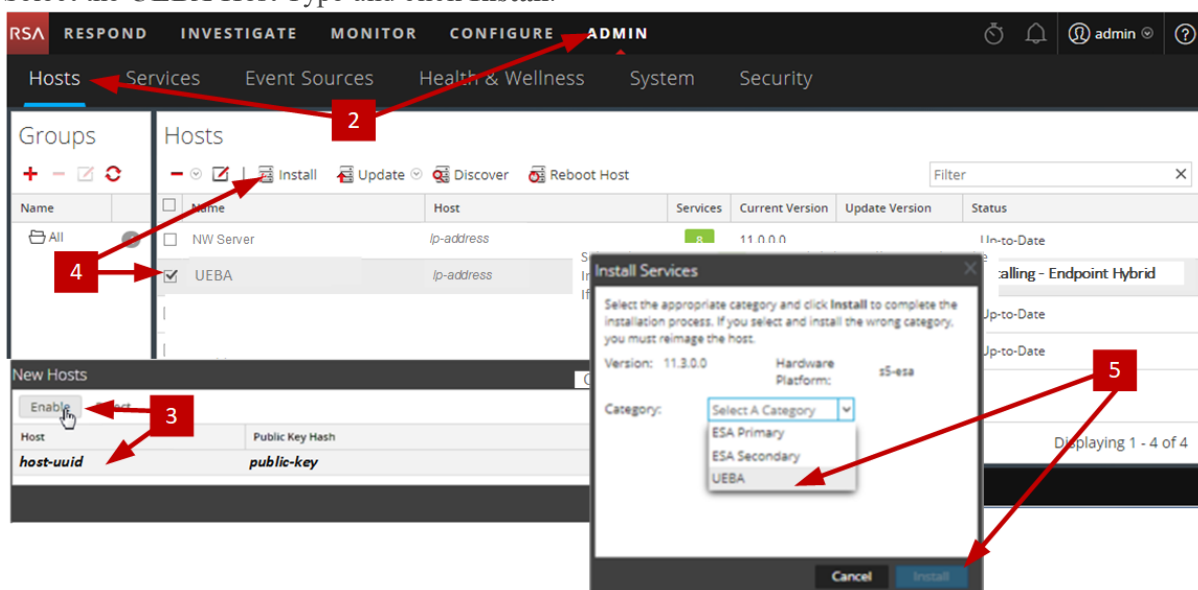
1. Complete steps 1 - 14 under "Task 2 - Install 11.3 on Other Component Hosts" in "Installation Tasks" of the *NetWitness Platform Physical Host Installation Guide for Version 11.3*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

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.

- Log in to 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.

- 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.
- Select that host in the **Hosts** view (for example, **UEBA**) and click  **Install**.
The Install Services dialog is displayed.
- Select the **UEBA** Host Type and click **Install**.




- Make sure that the UEBA service is running.
- Complete licensing requirements for NetWitness UEBA.
See the *NetWitness Platform 11.3 Licensing Management Guide* for more information. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

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.
You need to configure a data source (Broker or Concentrator), historical data collection start date, and data schemas.

IMPORTANT: If your deployment has multiple Concentrators, RSA recommends that you assign the Broker at the top of your deployment hierarchy for the NetWitness UEBA data source.

- a. Determine the earliest date in the NWDB of the data schema you plan to choose (AUTHENTICATION, FILE, ACTIVE_DIRECTORY, PROCESS, REGISTRY or any combination of these schemas) to specify in `startTime` in step c. If you plan to specify multiple schemas, use the earliest date among all the schemas. If you are not sure which data schema to choose, you can specify all five data schemas (that is, AUTHENTICATION, FILE, ACTIVE_DIRECTORY, PROCESS and REGISTRY) to have UEBA adjust the models it can support based on the Windows logs available. You can use one of the following methods to determine the data source date.
 - Use the Data Retention date (that is, if the Data Retention duration is 48 hours, `startTime` = <48 hours earlier than the current time>).
 - Search the NWDB for the earliest date.
- b. Create a user account for the data source (Broker or Concentrator) to authenticate to the data source.
 - i. Log into NetWitness Platform.
 - ii. Go to **Admin > Services**.
 - iii. Locate the data source service (Broker or Concentrator).

Select that service, and select  (Actions) > **View > Security**.
 - iv. Create a new user and assign the “Analysts” role to that user.

The following example shows a user account created for a Broker.

The screenshot displays the NetWitness UEBA Admin console interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN (selected). The ADMIN tab has sub-tabs for Hosts, Services, Event Sources, Health & Wellness, System, and Security. The left sidebar shows 'Change Service' and 'Broker' (selected). The main content area is divided into 'Users', 'Roles', and 'Settings' (selected). The 'Users' section shows a list of users with columns for Username, Broker, and admin. The 'Broker' user is selected. The 'User Information' section contains fields for Name (Broker), Username (Broker), Password, Confirm Password, Email (test@rsa.coim), and Description. The 'User Settings' section includes Auth Type (NetWitness Platform), Core Query Timeout (5), Query Prefix, and Session Threshold (0). The 'Role Membership' section shows a list of roles with checkboxes: Groups, Administrators, Aggregation, Analysts (checked), Data_Privacy_Officers, Malware_Analysts, Operators, and SOC_Managers.

Username	Broker	admin
Broker	Broker	
test@rsa.coim		

User Information

Name	Broker	Username	Broker
Password		Confirm Password	
Email	test@rsa.coim	Description	

User Settings

Auth Type	NetWitness Platform	Core Query Timeout	5
Query Prefix		Session Threshold	0

Role Membership

<input type="checkbox"/>	Groups
<input type="checkbox"/>	Administrators
<input type="checkbox"/>	Aggregation
<input checked="" type="checkbox"/>	Analysts
<input type="checkbox"/>	Data_Privacy_Officers
<input type="checkbox"/>	Malware_Analysts
<input type="checkbox"/>	Operators
<input type="checkbox"/>	SOC_Managers

- c. SSH to the NetWitness UEBA server host.

d. Submit the following commands.

```
/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.
-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> <p>!"#\$%&()*+,-.;<=>?@[\\]^_`{ }</p> <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' -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).
-t	<startTime>	<p>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).</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>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.</p> </div>

Argument	Variable	Description
-s	<schemas>	<p>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').</p> <p>Note: If you specify all five data schemas (that is, AUTHENTICATION, FILE, ACTIVE_DIRECTORY, PROCESS, and REGISTRY), UEBA adjusts the models it can support based on the Windows logs available.</p>
-v	NA	verbose mode.
-e	<argument>	<p>Boolean Argument. This enables the UEBA indicator forwarder to Respond.</p> <p>Note: If the Respond server is configured in NetWitness platform, you can transfer the NetWitness UEBA indicators to the respond server and to the correlation server to create an Incidents.</p>

9. Complete NetWitness UEBA configuration according to the needs of your organization. See the *RSA NetWitness UEBA User Guide* for more information. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

Note: If NetWitness Endpoint Server is configured, you can view the alerts associated with the Process and Registry data schemas.

For Virtual Hosts:

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

[Task 1. Install 11.3 on the NetWitness Server Host](#)

[Task 2. Install 11.3 Log Hybrid Host](#)

[Task 3. Install and Configure RSA NetWitness® UEBA](#)

Task 1. Install 11.3 on the NetWitness Server Host

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

- The 11.3.0.0 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 11.3.0.0 on the NW Server Host" section in the *Virtual Host Installation Guide for Version 11.3*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

Task 2. Install 11.3 Log Hybrid Host

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

- Install the 11.3.0.0 environmental platform.
- Apply the 11.3.0.0 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 11.3 for on Other Component Hosts" section in the *Virtual Host Installation Guide for Version 11.3*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents..

Task 3. Install and Configure RSA 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 11.3 on Other Component Hosts" in "Installation Tasks" of the *NetWitness Platform Physical Host Installation Guide for Version 11.3*. Go to the [Master Table of Contents](#) to find all NetWitness Platform Logs & Network 11.x documents.

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 RSA NetWitness® UEBA](#).

Post Installation Task

This topic contains the task you must complete after you install NetWitness UEBA standalone 11.3.

Set up Permission

You need to assign the UEBA_Analysts and Analysts roles to the UEBA users. For more information, see *System Security and User Management Guide*.

After this configuration, UEBA users can access the **Investigate > Users** view.

Appendix: NetWitness UEBA Standalone Installation

Windows Audit Policy

In order to achieve the maximum benefit from RSA NetWitness UEBA, RSA recommends that you implement the Windows audit policies described here.

For a base set of policies to audit, refer to the "Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008 Audit Settings Recommendations" section of this article from Microsoft: [Audit Policy Recommendations](#).

The policies under "Stronger Recommendation" are required, as well as the following policies, to ensure that all of the required Authentication and Active Directory events are audited:

- Audit Detailed File Share
- Audit File Share
- Audit File System

RSA recommends that you enable auditing for both success and failures.

The following Windows events must be audited:

For the Authentication models:

4624	4625	4769	4628
------	------	------	------

For the AD models:

4670	4717	4720	4722	4723	4724	4725	4726
4727	4728	4729	4730	4731	4732	4733	4734
4735	4737	4738	4739	4740	4741	4742	4743
4754	4755	4756	4757	4758	4764	4767	4794
5136	5376	5377					

For File Access Models:

4660	4663	4670	5145
------	------	------	------

Troubleshooting

Install Only One Instance of the NetWitness UEBA Server

RSA supports only one instance of the NetWitness UEBA server. If you have added more than one NetWitness UEBA server, follow these steps to remove the extra NetWitness UEBA server.

1. From the Admin server (node 0), run the following commands to query the list of installed NetWitness UEBA services:

```
# 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
```
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):

```
# orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output>
```
4. Run the following command to update node 0 to restore NGINX:

```
# orchestration-cli-client --update-admin-node
```
5. Log in to NetWitness Platform, go to **ADMIN > Hosts**, and remove the extra NetWitness UEBA host.

Contact Customer Support

Refer to the **Contact RSA Customer Support** page (<https://community.rsa.com/docs/DOC-1294>) in RSA Link for instructions on how to get help on RSA NetWitness Platform.