NetWitness® Platform XDR

Version 12.1

NetWitness UEBA Quick Start Guide

NETWITNESS

Platform XDR

NetWitness® Platform XDR

Version 12.1

NetWitness UEBA Quick Start 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

License Agreement

Third-Party Licenses

NETWITNESS
Platform XDR

NetWitness® Platform XDR

Version 12.1

NetWitness UEBA Quick Start Guide

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.

October, 2022

NETWITNESS
Platform XDR

What is NetWitness UEBA?

NetWitness UEBA (User and Entity Behavior Analytics) is an advanced analytics solution for discovering, investigating, and monitoring risky behaviors across all users and entities in your network environment. NetWitness UEBA is used for following reasons:

- Detecting malicious and rogue users
- Pinpointing high-risk behaviors
- Discovering attacks
- Investigating emerging security threats
- Identify potential attacker activity

About this Guide

This guide provides end-to-end instructions to configure NetWitness UEBA and to use UEBA features.

NetWitness Platform 11.7 Documentation in NETWITNESS community Link

NetWitness Platform product documentation is organized along functional lines. If you are looking for a specific guide or version, go to the Version 11.x Master Table of Contents.

Use these links to view the NetWitness Platform 11.5 documentation. Both links provide the same documentation, in these two formats:

- HTML Guides include the latest information for currently supported 11.x versions: NetWitness Platform 11.x Documentation.
- PDF Guides provide the information for a specific version: NetWitness Platform 11.7 PDFs.

Use these links to access documentation that is not related to a particular version of the software:

- Hardware setup guides: https://community.netwitness.com/t5/netwitness-platform-hardware/tkb-p/netwitness-hardware-documentation
- Documentation for Content such as feeds, parsers, application rules, and reports: https://community.netwitness.com/t5/threat-intelligence/ct-p/threat-intelligence.

Getting Started

The following tasks can be performed in any sequence.

Description	References
	
View information about product updates, improvements, and known issues.	Release Notes
Understand NetWitness UEBA	*NetWitness UEBA User Guide*

Setup and Installation

Standalone Installation

The following tasks must be performed in the following sequence.

Description	References
	
Review the supported hardware.	"System Requirement" topic in *UEBA Standalone Installation Guide*
Review the UEBA deployment.	"NetWitness UEBA Standalone Installation " topic in *UEBA Standalone Installation Guide*
Configure the ports on your firewall.	"NetWitness UEBA Standalone Installation " topic in *UEBA Standalone Installation Guide*
Install NetWitness Server host.	"Installation Tasks" topic in *UEBA Standalone Installation Guide*
Install 11.3 Log Hybrid Host.	"Installation Tasks" topic in *UEBA Standalone Installation Guide*
Install and Configure NetWitness UEBA.	"Installation Tasks" topic in *UEBA Standalone Installation Guide*
Assign the UEBA_Analysts and Analysts roles to the UEBA users.	"Role Permissions" in the System Security and User Management Guide

Fresh Installation

The following tasks needs to be performed in the following sequence.

Description	References
	
Review the supported hardware.	"Supported Hardware" in the *Physical Host Installation Guide*
Review the UEBA architecture.	"NetWitness Platform Network Architecture Diagram" topic in the *Deployment Guide*
Configure the ports on your firewall.	"Network Architecture and Ports" topic in the *Deployment Guide*
Install NetWitness Server host and other components.	"Task 1 - Install 11.7 on the NetWitness Server (NW Server) Host" and "Task 2 - Install 11.7 on Other Component Hosts" in *Physical Host Installation Guide* "Install NetWitness Platform Virtual Host in Virtual Environment" in the *Virtual Host Installation Guide*
Install UEBA.	"NetWitness® UEBA" in *Physical Host Installation Guide*
Assign the UEBA_Analysts and Analysts roles to the UEBA users.	"Role Permissions" in the *System Security and User Management Guide*

Update

The following tasks must be performed in the following sequence.

Description	References
	
Deploy the Endpoint Pack from Live, which contains File Category Lua Parser for the UEBA integration with Endpoint.	During deployment, you must specify Endpoint Log Hybrid Log Decoder service. In case of multiple Endpoint servers, select all the Endpoint Log Hybrid Log Decoder services
Enable Endpoint data sources such as Process and Registry to generate alerts in UEBA.	"Enable Endpoint Data Sources" in the *Update Instructions*
Enable UEBA indicator forwarder to transfer the UEBA indicators to the NetWitness Respond server and to the correlation server to create an incidents.	"Enable UEBA Indicator Forwarder" in the *Update Instructions*

Description	References
After you update to NetWitness Platform 11.7 the Broker or Concentrator UUID changes. You must update the NetWitness Platform core services, and update the Broker or Concentrator UUID.	"Update Broker or Concentrator UUID" in the *Update Instructions*
Update Airflow Configuration.	"Update Airflow Configuration" in the *Update Instructions*
Restart the Airflow scheduler service after the presidio_ upgrade DAG is successful.	"Restart Airflow scheduler service" in the *Update Instructions*

Investigation

The following tasks can be performed in any sequence.

Description	References
	
Investigate high risk users.	"Investigate High-Risk Users" topic in the *NetWitness UEBA User Guide*
Investigate top alerts.	"Investigate Top Alerts" topic in the *NetWitness UEBA User Guide*

Monitoring

The following tasks can be performed in any sequence.

Description	References
	
Review NetWitness UEBA metrics in Health and Wellness.	"View NetWitness UEBA Metrics in Health and Wellness" topic in the NetWitness UEBA User Guide
Monitor Health and Wellness of UEBA.	"Monitor Health and Wellness of UEBA" topic in the NetWitness UEBA User Guide