



Nuix Adaptive Security

Nuix Adaptive Security 2.16.3

Release Notes

August 2023



Copyright © 2023 Nuix. All rights reserved.

This publication is intended for informational purposes only. The information contained herein is provided “as-is” and is subject to change without notice. Although reasonable care has been taken to ensure that the facts stated in this publication are accurate, no representation or warranty, expressed or implied, is made as to the fairness, accuracy or completeness of the information.

Nuix (and any other Nuix trademarks used) are trademarks of Nuix Ltd. and/or its subsidiaries, as applicable. All other brand and product names are trademarks of their respective holders. Any use of Nuix trademarks requires prior written approval from the Nuix Legal Department. The Nuix Legal Department can be reached by e-mail at Legal@nuix.com.

THIS MATERIAL IS COMPRISED OF INTELLECTUAL PROPERTY OWNED BY NUIX LTD. AND ITS SUBSIDIARIES (“NUIX”), INCLUDING COPYRIGHTABLE SUBJECT MATTER THAT HAS BEEN NOTICED AS SUCH AND/OR REGISTERED WITH THE UNITED STATES COPYRIGHT OFFICE. ANY REPRODUCTION, DISTRIBUTION, TRANSMISSION, ADAPTATION, PUBLIC DISPLAY OR PUBLIC PERFORMANCE OF THE INTELLECTUAL PROPERTY (OTHER THAN FOR PREAPPROVED INTERNAL PURPOSES) REQUIRES PRIOR WRITTEN APPROVAL FROM NUIX.

The use, reproduction, and/or distribution of any Nuix software described in this publication requires an applicable software license.

Contents

Introduction	1
About Nux Adaptive Security	1
Product documentation	1
Fixed issues	2
Known issues	2
Supported upgrade paths	2

Introduction

This document provides an overview of Nuix Adaptive Security's new features, resolved issues, and known issues.

About Nuix Adaptive Security

Visibility into the security of your environment is crucial to your organization's success. Nuix Adaptive Security can help you answer questions about your organization, such as:

- Is my organization compromised?
- Has someone taken critical data out of my organization?
- How was someone able to access our environment?
- Is something about to happen?

When you don't have visibility, it leaves your organization in a precarious position, at a decision-making disadvantage, and open to greater risk.

Nuix Adaptive Security delivers a proactive approach that provides the kind of *visibility*, *adaptability*, and *control* that is missing with traditional endpoint products. By leveraging endpoint analytics, Nuix Adaptive Security reduces the time it takes to detect an impending or ongoing attack, accelerates recovery time, easily adapts to changing environments, regulations, and attack vectors, and ultimately, stops incidents in their tracks.

Nuix Adaptive Security has perfected the art of continuous monitoring and response to isolate the important (and often small) signals from the noise and identify when behaviors exhibit uncharacteristic patterns. Nuix Adaptive Security relies on two fundamental and unique elements to drive the *protect-detect-response-remediate* process:

- The Digital Behavior Recorder (™) continuously monitors and records key digital behaviors.
- The patent-pending logic engine provides customizable logic on the endpoint, enabling it to recognize and act on threats in real time.

Product documentation

The following documents comprise the Nuix Adaptive Security documentation set for this version of the product:

- Nuix Adaptive Security Release Notes, Version 2.16.3 (this document)
- Nuix Adaptive Security Rule Language Reference Guide, Version 2.16.0
- Nuix Adaptive Security Installation Guide, Version 2.16.1
- Nuix Adaptive Security Quick Start Guide, Version 2.16.0
- Nuix Adaptive Security User Guide, Version 2.16.1
- Nuix Adaptive Security Administration Guide, Version 2.16.0

Fixed issues

This section lists the fixed issues in this release.

- Right-click and Collect were not working for Linux. This is now fixed.
- The Day and Month displayed bugs when using a UK system. This is now fixed.
- Applied fixes to the Win7 32-bit agent.
- Updated the Mac and Linux endpoints to improve the size of a file that they can collect.
- Added Agent support for RHEL 7.
- Added a few new sample rules.
- Added updates to some of the third-party libraries on the server.
- Enhanced the error handling for agent application hooking.

Known issues

This section lists the known issues identified in this release.

- On a multi-server installation, if one of the secondary servers is not running, the application UI could become sluggish or non-responsive.
- When the primary server has the firewall enabled, the replication of the configuration to the secondary servers does not work.
 - In non-AWS environments, every time a secondary server is added, modify the firewall on the primary server so that incoming connections to high ports are opened to the Adaptive API service from all of the secondary servers.
 - In AWS environments, the security group for the primary server should allow incoming connections to all high ports from the security group assigned to the secondary servers.
- When you select to download a file or screenshot, the files are saved in a password-protected zip file. The standard Windows 10 unzip tool does not support AES256 encryption used by Nuix Adaptive Security. You will need a third-party tool, such as 7-zip, to extract the files.
- URL monitoring on the Linux agent might not always work because the Linux agent does not always detect that a browser process is launching.
- The agent upgrade task does not go out when the Hash list is set to None in the Configuration. When the user attempts to upgrade an agent and selects 'None' for the Hash Configuration the upgrade will fail. The user can leave the hash list field empty, and the agent upgrade will be successful.

Supported upgrade paths

You can upgrade the following versions of Nuix Adaptive Security to 2.16.3:

- Nuix Adaptive Security 2.16.0
- Nuix Adaptive Security 2.14.0
 - When upgrading from version 2.14 to 2.16.1 you must uninstall the microservices before starting the upgrade process.

For more about upgrades, see the *Nuix Adaptive Security Installation Guide*.