



FortiNAC - Release Notes

Version 8.7.1

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



February 02, 2020

FortiNAC 8.7.1.1505 Release Notes

49-871-608787-20200203

TABLE OF CONTENTS

Overview of Version 8.7.1	4
Important	4
Supplemental Documentation	4
Version Information	4
Compatibility	6
Agents	6
Web Browsers for the Administration UI	6
Operating Systems Supported Without an Agent	7
New Features in 8.7.1	8
New Features in 8.7.0	9
FortiAnalyzer Integration	9
Corporate Security Fabric Protocol	9
Excluded MAC Address Ranges	9
Rest API	9
Additions	9
Enhancements and Addressed Issues	10
Version 8.7.1.1505	10
Version 8.7.0.1503	11
Device Support	12
Version 8.7.1.1505	12
Version 8.7.0.1503	12
System Update Settings	14
End of Support/End of Life	15
End of Support	15
Agent	15
Software	15
Hardware	15
Appliance Operating System	15
End of Life	16
Software	16
Numbering Conventions	17

Overview of Version 8.7.1

Version 8.7 is the latest release being made available to customers to provide functionality and address some known issues.

Important

- Prior to upgrade, review the FortiNAC Known Anomalies posted in the [Fortinet Document Library](#).
- If using agents or configured for High Availability, additional steps may be required after upgrade for proper functionality. See [Upgrade Instructions and Considerations](#) posted in the Fortinet Document Library.
- Requires CentOS 7.4 or higher. The current CentOS version installed is listed as "Distribution" in the CLI login banner or typing "sysinfo".
Example:

```
> sysinfo
*****
Recognized platform: Linux
Distribution: CentOS Linux release 7.6.1810 (Core)
If the CentOS version is below 7.4, run OS updates and reboot before upgrading. For instructions on updating CentOS, refer to the Fortinet Document Library.
```
- For upgrade procedure, see [Upgrade Instructions and Considerations](#) posted in the Fortinet Document Library.

Supplemental Documentation

The following can be found in the [Fortinet Document Library](#).

- 8.x Fixes and Enhancements Summary
- FortiNAC Release Matrix

Version Information

These Release Notes contain additional Enhancements, Device Support, and features. Unique numbering is used for the various components of the product. The software version and Agent version supplied with this release are listed below.

Version: 8.7.1.1505

Agent Version: 5.2.1.8

A newer Persistent Agent may be required to support certain antivirus and anti-spyware products. Refer to the Agent Release Notes in the [Fortinet Document Library](#).

Firmware version represents a collection of system services and operating system features imaged on to the appliance before it leaves manufacturing. The firmware image cannot be updated by a Fortinet customer. Services within the image are updated by Fortinet or a certified Fortinet Partner in appliance maintenance packages released as new more robust and secure versions of services become available.

Note that upgrading software versions does not change firmware nor does it automatically require an upgrade to the Persistent Agent. Newer Persistent Agents are not compatible with older software versions unless that capability is specifically highlighted in the corresponding release notes.

Compatibility

FortiNAC Product releases are not backwards compatible. It is not possible to go from a newer release to any older release.

Example: 8.1.1.132 cannot be downgraded to any other release.

To backup the current system prior to upgrade on virtual machines, perform a snapshot. For physical appliances refer to the document Back Up and Restore an Image of a FortiNAC Appliance.

Agents

FortiNAC Agent Package releases 5.x are compatible with FortiNAC Product release 8.x. Compatibility of Agent Package versions 4.x and below with FortiNAC versions 8.x and greater are not guaranteed.

Web Browsers for the Administration UI

Safari web browser version 6 or greater

Google Chrome version 26 or greater

Mozilla Firefox version 20 or greater

Internet Explorer version 9.0 or greater

Opera version 12.15 or greater

Many of the views in FortiNAC are highly dependent on JavaScript. The browser used directly impacts the performance of these views. For example, the new Host view in one browser may take 2 seconds to load, but the same view in a different browser may take 20 seconds. To improve performance, it is recommended that you choose a browser which is fast at processing JavaScript, such as, Google Chrome. Articles on comparing the performance of various web browsers are freely available on the internet. Some performance sites include:

- <http://legitreviews.com/article/1347/1/>
- <http://w-shadow.com/blog/2010/04/20/web-browser-performance-comparison/>
- <http://sixrevisions.com/infographs/browser-performance/>
- <http://w-shadow.com/blog/2010/11/03/browser-performance-comparison/>

If your browser is not optimized for processing JavaScript, you may see an error message display when accessing a view that uses JavaScript. The message will vary depending on your browser.

Example:

Warning: Unresponsive script

A script on this page may be busy, or it may have stopped responding. You can stop the script now or you can continue to see if the script will complete.

Script: http://<IP>/js/yui/yahoo-dom-event/yahoo-dom-event.js:8"

Operating Systems Supported Without an Agent

Android	Apple iOS	Blackberry OS	BlackBerry 10 OS
Chrome OS	Free BSD	Kindle	Kindle Fire
iOS for iPad	iOS for iPhone	iOS for iPod	Linux
Mac OS X	Open BSD	Net BSD	RIM Tablet OS
Solaris	Symian	Web OS	Windows
Windows CE	Windows Phone	Windows RT	

New Features in 8.7.1

There are no new features in 8.7.1.

New Features in 8.7.0

FortiAnalyzer Integration

FortiNAC Analytics is replaced by FortiAnalyzer for endpoint and network infrastructure reporting.

Corporate Security Fabric Protocol

Added support for the Corporate Security Fabric Protocol so that FortiNAC can be registered as a Security Fabric appliance in FortiOS Security Fabric tree. FortiNAC appliances will then be visible in the Security Fabric Topology view on FortiOS products. This function is configured under **System > Settings > System Communication > Fortigate Telemetry**.

Note: Requires FortiNAC appliances to be installed with licenses that include certificates. This type of license was introduced January 1st 2020.

Excluded MAC Address Ranges

The Excluded MAC Address Ranges feature is removed from the GUI. Excluding Microsoft LLTD and Multicast Addresses is still supported.

Rest API

Rest API enhancements made for later GUI-rewrite.

Additions

- FortiGate VPN support
- New profiling method for ONVIF protocol support
- Entitlements will display in the License Information panel of the dashboard

Enhancements and Addressed Issues

These changes have been made in FortiNAC Version 8.7.1. These enhancements are in addition to the enhancements that are outlined in 8.6 and previous releases.

Version 8.7.1.1505

Ticket #	Description (8.7.1.1505)
3688356	Fixed HPE OfficeConnect 1950-48G VLAN change method
	Changed Google GSuite integration to read the most recently logged in user by default.
	Changed Google GSuite polling to ignore serial numbers greater than 255 characters
3683450 3734952	Fixed issue where topology devices were not assigned Network Device Roles
3683024	Resolved issue where SnmpEventThreads were stuck waiting for L2 Polls
3579417	FortiNAC now deletes the groups when the conference is either deleted automatically or when an admin deletes it.
	Fixed NullPointerException
3746264	Fixed issue where Settings > Credential Configuration > Persistent Agent > RADIUS/LDAP used Local instead of LDAP. Previously, the Persistent Agent did not register hosts when this option was selected.
	Added Security Actions to System > Groups > In Use
	Changed the field Serial Number if FortiAnalyzer is selected as a type in Log Receivers.
	Fixed remove group method
3743521 3762737	Fixed a bug that prevented setting the port in the WinRM method configuration of Device Profiling Rules.
3539756	Fixed sync issues with pods due to duplicate groups
	Fixed distribute of updates from NCM to pods. Previously, attempting to use the Distribute button in the NCM Administration UI would fail with a 500 error code.
	Fixed issue where PA Communication flag was not consistently set and unset.
	Fixed issue with VLAN reads and VLAN switching for Aruba SSeries DLink and HP WX Wireless

Version 8.7.0.1503

Ticket #	Description (8.7.0.1503)
2969968	Fixed issue with populating a default set of networks and profiles. Previously, when no Logical Networks were configured, the method to populate the default networks/profiles failed.
	Fixed broken document link in GUI
	Removed the subnet from the FortiNet FSSO Settings
	Added support for reading and writing Unicode values. This allows Polish characters to display properly in the Administration UI.
	Added support for LLDP to device discovery
	Added <code>-loggers</code> mode to CampusMgrDebug
	Fixed issue where Security Alarms were created with a delay
	Removed the Excluded MAC Address Range feature. Only the Exclude Microsoft LLTD Addresses and Exclude Multicast Addresses will be supported
	The "Last Name" of a User is no longer required to be non-empty. This includes local Users and LDAP users.
	Made changes to license scheme for hardware
	Added RADIUS support for wired ports on FortiSwitches operating in FLink mode.
	Further integrated FortiNAC with FortiAnalyzer as new reporting tool. Added ability to send endpoint and infrastructure data to FortiAnalyzer in order to build reports.
	Fixed issue so that IP Phone does not send port-based CLI to device if no enforcement is enabled.
	Fixed issue where starting device discover produced an HTTP 500 Internal Server Error
	Improved speed performance of NCM CLI Filter reports

Device Support

These changes have been made in FortiNAC Version 8.7.1. These are in addition to the device support added in 8.6 and previous releases.

Version 8.7.1.1505

Ticket #	Vendor
3531712	Cisco
3457026	
3620676	
3690680	
3431702	
	FortiSwitch
3746463	HP
3584288	Ubiquity UniFi Wireless
3725210	

Version 8.7.0.1503

Ticket #	Vendor (8.7.0.1503)
	Alcatel
	Aruba
3550729	Cisco
3556085	
3437522	
3411005	
3515941	
3671084	
	Dell
	DLink
	Extreme

Ticket #	Vendor (8.7.0.1503)
	FortiGate 101E and 600E
	Foundry
	H3C
	HP
	HPE
	Juniper

System Update Settings

Use the following System Update Settings when upgrading through the Administrative UI:

Field	Definition
Host	Set to update.bradfordnetworks.com
Directory or Product Distribution Directory	Systems running version 8.3.x and higher: Set to Version_8_7 Systems running version 8.2.x and lower: Set to Version_8_7_NS
User	Set to updates (in lowercase)
Password	Keep the current value.
Confirm Password	Keep the current value
Protocol	Set to desired protocol (FTP, PFTP, HTTP, HTTPS) Note: SFTP has been deprecated and connections will fail using this option. SFTP will be removed from the drop down menu in a later release.

End of Support/End of Life

Fortinet is committed to providing periodic maintenance releases for the current generally available version of FortiNAC. From time to time, Fortinet may find it necessary to discontinue products and services for a number of reasons, including product line enhancements and upgrades. When a product approaches its end of support (EOS) or end of life (EOL), we are committed to communicating that information to our customers as soon as possible.

End of Support

Agent

Versions 2.x and below of the Fortinet Agent will no longer be supported. FortiNAC may allow the agent to communicate but functionality will be disabled in future versions. Please upgrade to either the Safe Harbor or latest release of the Fortinet Agent at your earliest convenience.

Fortinet Mobile Agent for iOS will no longer be supported. It will be completely removed in a future version. EasyConnect features are not affected as they do not require an agent on iOS.

Software

When a code series has been announced End of Support, no further maintenance releases are planned. Customer specific fixes will still be done.

Hardware

Physical appliance hardware reaches end-of-support when the maintenance contract is non-renewed, or at the end of year 4 (48 months beyond purchase date), whichever is first.

Appliance Operating System

Fortinet relies on the CentOS organization to publish periodic bug fixes and security updates for the CentOS Distribution.

CentOS 5

Effective March 31, 2017, CentOS will no longer provide updates for CentOS 5. Any vulnerabilities found with CentOS 5 after March 31st will not be addressed. FortiNAC software releases will continue to be supported on CentOS 5 through December 31, 2018.

As of 2016 Fortinet's appliances are based on the CentOS 7 Linux distribution. New appliance migration options are available for customers with CentOS 5 appliances who require operating system vulnerability patches, maintenance updates and new features available on CentOS 7.

CentOS 7

Effective June 30 2024, CentOS will no longer provide updates for CentOS 7. Any vulnerabilities found with CentOS 7 after June 30th will not be addressed.

FortiNAC and Analytics software releases will continue to be supported on CentOS 7 through December 31 2026 or end of product life (whichever comes first). See Product Life Cycle chart for details.
(<https://support.fortinet.com/Information/ProductLifeCycle.aspx>)

End of Life

Software

When a code series has been announced End of Life, no further maintenance releases are planned. In addition, customer specific fixes will not be done. If experiencing problems with a version of FortiNAC in the code series, you would be required to update before any issues can be addressed.

With the release of FortiNAC Version 8.5.0, Fortinet announced the End-Of-Life for FortiNAC 8.1. Existing customers under maintenance are strongly encouraged to upgrade to the current Safe Harbor release.

Considerations are as follows:

- FortiNAC Versions 7.0 and higher are not supported on appliances running firm -ware Version 2.X (SUSE) because of the limitations of this operating system and the hard ware on which it is installed. Please contact your sales representative for hardware upgrade options.
- If you attempt to install FortiNAC Versions 7.0 and higher on an unsupported Operating System and hardware combination, the install process displays the following message: "This release is not supported on 1U SUSE Linux appliances (firmware 2.x). The install process will exit now. Please contact Fortinet at: +1 866.990.3799 or +1 603.228.5300"
- On July 13, 2010 Microsoft ended support for Windows 2000 and Windows 2000 Server. These Operating Systems will be removed from the list of options in the Scan Policy Configuration screens in a future release.

Numbering Conventions

Fortinet is using the following version number format:

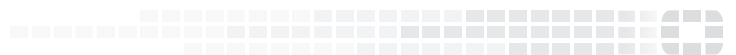
<First Number>.<Second Number>.<Third Number>.<Fourth Number>

Example: 8.0.6.15

- First Number = major version
 - Second Number = minor version
 - Third Number = maintenance version
 - Fourth Number = build version
-
- Release Notes pertain to a certain version of the product. Release Notes are revised as needed. The Rev letter increments accordingly. For example, updating the Release Notes from Rev C to Rev D indicates changes in the Release notes only -- no changes were made to the product.
 - The next number represents the version in which a Known Anomaly was added to the release notes (for example, V8.0).



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.