FortiNAC - Release Notes

Version 8.6.1

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

September 25, 2019
FortiNAC 8.6.1 Release Notes
49-861-585543-20190925

TABLE OF CONTENTS

Overview of Version 8.6.1

Version 8.6 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 carious components of the product. The software version and Agent version supplied with this release are listed below.

Version: 8.6.1

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 asnew 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 8.6.1

Self Registration Auto-fill

An LDAP lookup searches for matching sponsors as the Sponsor field is filled out in the Guest Self Registration page of the FortiNAC captive portal. This function can be used to auto-fill the entry and displays matching searches' full name and email address. What is displayed is configurable so that the email address is not shown.

New Features in 8.6.0

Nozomi Networks Integration

What it does:

- Expands device Trust in FortiNAC to those devices managed by Nozomi appliances. This also further extends FortiNAC's endpoint visibility of managed devices.
- Security event parsing for Automated Threat Response

For integration instructions, refer to the Fortinet Document Library.

Dot1x Auto Registration

What it does:

Automatic registration of a host based upon the user's 802.1x authentication with the RADIUS server. The feature is enabled/disabled in the SSID Configuration view of the Controller/Access Point model under Network Devices > Topology.

Enhanced Visibility by Leveraging Traffic Analysis

What it does:

- FortiGate session information is pulled and saved based on endpoint models in FortiNAC.
- Rogue / Unknown Endpoint host records can now be created based upon the presence of the endpoint's MAC Address in the Fortigate session table or a router's ARP table.
- FortiGate Sessions View
  - Allows an admin to view endpoint connections and to build profiling rules from the information.

  See FortiGate sessions in the Administration Guide for more information.
- New Device Profiling Methods
  - Network Traffic (Network Flow)
    - Identify / Classify device based on traffic
    - Protocol / Application, Source, Destination
  - FortiGate
    - Classify based on device type from FortiGate
    - Classify based on Hostname, Device Type

    See Device Profiler - Adding a rule in the Administration Guide for more information.

Unique Device ID

This feature creates a unique ID for the endpoint based on hardware attributes.

UI Default Theme

The default theme for the UI is now green.

Enhancements and Addressed Issues

These changes have been made in FortiNAC Version 8.6.1. These enhancements are in addition to the enhancements that are outlined in 8.5 and previous releases.

Version 8.6.1

Ticket #	Description (8.6.1)
	Fixed misleading error message displayed in the Network Control Manager when Administrative user didn't have permissions to Sync to the remote appliance.
	Fixed RADIUS authentication problems when VendorSpecificAttributes are used which have no data.
	Fixed problem where the SSID was not showing for Aruba IAP
3442935	Fixed VLAN switching on FortiSwitch ports when FortiSwitch is managed by FortiGate and multiple VDOMs are configured
3442941	Fixed ARP reads from FortiGate devices to avoid stale entries
3338013	Fixed problem where monitor results for a scan override other monitor results
3454556	Fixed issue with sending SSO information to PaloAlto
3469011	Fixed problem when synchronizing credentials for WMI Profile method of Device Profiling Rules
	Added feature where hosts discovered by Microsoft InTune polling are added to a group by default.
2989037 3456547	Added VRF support for more Passport Devices
	Fixed issue where DirectoryAuthentication SQL Exception was thrown during startup with an initial database.
2969900	Fixed L2 polling issue for Aruba where wireless client status showed online for offline clients after polling.
3439673	Fixed bug that prevented saving SSO Agent configuration with a PLUS license
3437941 3446737 3450676 3482984	Fixed L2 polling issue with large Aruba controller deployments

Ticket #	Description (8.6.1)
	Fixed an issue with socket leaks
3448792	Fixed problem that prevented executing database backup after modifying schedule
	Added new feature in Self Registration that allows sponsors to be looked up from LDAP within a supplied group
3425086	Fixed issue with synchronization of Access Policy related configuration from the FortiNAC Manager
	Fixed syncing issue when deleting a Logical Networks from NCM
3437941 3446737 3450676 3482984	Fixed L2 polling for Aruba controllers running 8.5.x firmware.
	Modified the behavior of revalidation settings in Device Profiling rules so that settings changed in the rule are mirrored in the host record
	Fixed issue with starting secondary control server after reboot
3398171	Fixed problem affecting AP creation for Cisco WLC devices
3432022 3459920	Fixed file permissions for /bsc/siteConfiguration/apache_ssl
3433571	Fixed the setting "Send to External Log Hosts" in Event to Alarm Mappings view
	Updated legal page to reflect change from Oracle JDK to OpenJDK
3393612 3444637	Fixed the redirect URL format for MS InTune Integration authentication
	Added support to Device Profiler for some difficult to match Windows DHCP INFORMS
	Added support for Link Layer Discovery Protocol to device discovery
	Fixed issue where changing the Agent Contact Window on Host Disconnect setting from its default of 30 seconds did not take effect. Added inline help text.
3391677	Fixed missing property in the portal's EasyConnect Success page which displayed as `??Common.context??`
	Sanitized and removed multiple files for CWE-78
	Consolidated startCMProcesses and startupCMRCProcesses for easier maintenance
3402843	Fixed potential NTP configuration bug in the Configuration Wizard

Version 8.6.0.320

Ticket #	Description (8.6.0.320)
	Added FlexCLI support for Juniper Switches
	Added the container attribute to Endpoint REST API queries
	Fixed ARP parsing for two Brocade switches (FWS624-POE and FWS648-POE)
3323458	Network Access configuration and in Switch Model Configuration, only the first 25 are shown.
3233019	Network Device Roles can now specify a Logical Network.
3247036	Security event is not triggering an alarm despite correct configuration
	Exception thrown when attempting to run a policy test.
3102103	Fixed issue with intermittent endpoint connections and agent connection status.
	When using "Advanced Scan Controls" in an EPC Configuration, "Security Risk Host" and "Host Passed Security Test" will now be generated.
	Export/Import profile rules for profiled device.
	In the device profiling rules, separated the icon type from the "Match Type" in the profiling methods.
3308700	Fixed issues updating host via API
	Allow administrators to specify the RSA key length in Cert Management
	Allow multiple, unrelated Certificate Authorities (CAs) in trusted cert targets
	Events for Policy/Configuration/Profile modifications are not generated.

Ticket #	Description (Fixed in 8.6.0.320 and 8.5.2.665)
	Moved default Device Profiling rule "APC - UPS" to be ranked last
	Fixed file permission issue on application servers.
	Fixed file permission error for /etc/httpd/conf.d/000_web_services.conf on application server
	Added example ServiceNow integration script
	Added additional error messages to the WMI Profile Device Profiling method.
	Fixed duplicate Database Archive Help bubble
	Local documentation has been removed and replaced with the Fortinet Documentation Library.
3379993 3359349	Fixed problem connecting to LDAP servers via SSL after upgrade when not connecting by name.
3380684	Fixed problem where credentials of existing devices could be modified by discovery process.
	NullPointerException in DHCPMethodData
3187751	Fixed hosts that register via Captive Portal losing Vendor Name
	Fixed Settings -> Syslog Files when licensed for FortiNAC Plus.
3352649	FNC is now tolerant of Cisco WLC SSID/WLAN names containing trailing whitespace.

Device Support

These changes have been made in FortiNAC Version 8.6.1. These are in addition to the device support added in 8.5 and previous releases.

Version 8.6.1

Ticket #	Vendor
	Aruba
	Cisco
	Dell
	D-Link
	HPE
	HPN

Version 8.6.0.320

Ticket #	Vendor (8.6.0.320 and 8.5.2.665)
	Alcatel-Lucent
3374474	Cisco
	Dell
	ForiWifi
	H3C
3376454	HP H3C
3388813	HPE
	Huawei
2969110	Juniper
	Meraki
	Ruckus/Brocade
	Ruckus

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_6** Systems running version 8.2.x and lower: Set to **Version_8_6_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.

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).

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.