



# FortiNAC - Release Notes

Version 8.7.6

**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/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



October 12, 2020

FortiNAC 8.7.6.1523 Release Notes

49-876-670332-20201012

---

# TABLE OF CONTENTS

<b>Overview of Version 8.7.6</b>	<b>5</b>
Important	5
Supplemental Documentation	5
Version Information	5
<b>Compatibility</b>	<b>7</b>
Agents	7
Web Browsers for the Administration UI	7
Operating Systems Supported Without an Agent	8
<b>New Features in 8.7.6</b>	<b>9</b>
<b>New Features in 8.7.5</b>	<b>10</b>
<b>New Features in 8.7.4</b>	<b>11</b>
<b>New Features in 8.7.2</b>	<b>12</b>
<b>New Features in 8.7.1</b>	<b>13</b>
<b>New Features in 8.7.0</b>	<b>14</b>
FortiAnalyzer Integration	14
Corporate Security Fabric Protocol	14
Excluded MAC Address Ranges	14
Rest API	14
Additions	14
<b>Enhancements and Addressed Issues</b>	<b>15</b>
Version 8.7.6.1523	15
Version 8.7.5.1519	16
Version 8.7.4.1517	18
Version 8.7.2.1513	19
Version 8.7.1.1505	23
Version 8.7.0.1503	24
<b>Device Support</b>	<b>26</b>
Version 8.7.6.1523	26
Version 8.7.5.1519	26
Version 8.7.4.1517	27
Version 8.7.2.1513	27
Version 8.7.1.1505	28
Version 8.7.0.1503	29
<b>System Update Settings</b>	<b>30</b>
<b>End of Support/End of Life</b>	<b>31</b>
End of Support	31
Agent	31
Software	31
Hardware	31
Appliance Operating System	31

---

End of Life .....	32
Software .....	32
<b>Numbering Conventions .....</b>	<b>33</b>

## Overview of Version 8.7.6

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:** 8.7.6.1523

**Agent Version:** 5.2.4

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 8.7.6

There are no new features in 8.7.6.1523.

## New Features in 8.7.5

There are no new features in 8.7.5.1519

## New Features in 8.7.4

There are no new features in 8.7.4.1517

## New Features in 8.7.2

There are no new features in 8.7.2.

## 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 8.7.6. These enhancements are in addition to the enhancements that are outlined in 8.6 and previous releases.

### Version 8.7.6.1523

Ticket #	Description (8.7.6.1523)
588568	Container field only updates on a reconnect to the network
593600	Discovery slow in NCM environment
595663	Cisco Sx300 RADIUS support
610335	Role retrieved from WindowsAD Group changes when directory sync is run. Affects user accounts that are in multiple AD groups, regardless if Distinguished Name (DN) is different.
626560	Controller managed Aruba APs are incorrectly updated with IP of 0.0.0.0
640596	After changing existing eth0 IP address configuration using configIP tool and applying configWizard, system is changed from standalone to HA configuration.
644734	Devices in Topology View shows as rogue devices on FGT Interface
645982	OS Updates currently defaults to FTP but customers prefer HTTP
646470	New host/adaptor records fail to create when new client connects and managing FortiGate is configured for Syslog messaging. Affects clients connecting to FortiSwitches in Link mode and directly to FortiGate.
649550	Support for FortiGate Device Detection trap
650618	Read IPv6 arp issues.FortiNAC showing the IPv6 link local address and not the IPv4 address.
651375	Improved Cisco WS-C3850 mapping as hybrid wired/wireless device.Corrected issue where existing Cisco WS-C3850 switches used for wired only no longer worked properly after upgrade to 8.7.5 or 8.8.1. Note: This device model now appears in Topology as a wireless model since it can act as both a switch and wireless device.
656100	Internal Server Error 500 pop-up when saving modified LDAP settings
656123	Port substitution inserts wrong format for Dell switches.Affects CLI communication between FNAC and switch (such as Flex CLI).
656492	FortiGate 100F on FortiNAC 8.7.4 discovered as a FortiGate 100E

Ticket #	Description (8.7.6.1523)
656763	FortiNAC sending FSSO messages to unexpected FortiGates
659006	Improved device support for Motorola/Extreme wireless devices versions greater than 5.x
660275	Rogues are unable to connect to wireless network due to slow processing.
661500	In MS Intune integrations, FortiNAC does not display an owner for hosts whose e-mail prefix do not match the directory user ID.
661753	Dissolvable Authentication process loops when usernames with different case between external authentication source (like Google) and another (like LDAP).
661759	Dissolvable Agent, errors in handling are reported as Success to the user.
663058	When re-scanning host using the Dissolvable Agent, a "Login failed" error displays.
663486	LDAP search filters not working correctly with non-ASCII characters.
663497	FortiNAC generated telnet results in malformed packet
663502	Added support for newer Cisco WLC devices that have enable passwords configured.
664301	Rogue DHCP Server Detection not working
665244	iOS MAC randomization is now disabled through the application of a Supplicant Configuration. This requires configuring an EasyConnect policy to match iOS devices during registration.
665680	Device Profiler mapped Cisco IOS as Mac OS X
666543	L3 HA: Secondary (In Control) replies to DNS inquiries with Primary (Not In Control) ETH1 IP address.
666556	Null Pointer Exception in Device Server when debug is enabled
668607	FortiNAC may not have permission to read/write /etc/dhcp/dhcpd.conf after OS updates
668952	Method calls from a pod to the NCM over CORBA are prone to hanging
669166	Multiple Devices required support via email
669449	FNAC is sending FSSO tags incorrectly to uninitialized FGTS.

## Version 8.7.5.1519

Ticket #	Description (8.7.5.1519)
557253	ARP entry for Virtual IP (VIP) is not updated after L2 High Availability



Ticket #	Description (8.7.5.1519)
520262	failover.
588289	A single SSH/Telnet session is now used to read all VRFs on Passport VSP routers
600359	Hosts registering using Anonymous Authentication do not change networks until the next L2 Poll occurs
638109	Vulnerability Scanner integration with Tenable/Nessus not functioning due to new API with authentication changes
638810	Incomplete ARP(IP -> MAC) information when L3 polling FortiGates with multiple VDOMs.
640852	Inaccurate L2 information when authentication is enabled on Alaxala switches
644627	Clients connecting over VPN do not always get presented with the VPN context in Captive Portal
647181	Windows device profile not parsing correctly, causing a failed match
647193	Logging on a User does not trigger a VLAN Switch until a L2 Poll
647211	FNAC not sending user information to Palo Alto firewalls. This prevents User-ID information from appearing in the Palo Alto logs when integrated with FNAC.
647674	Voice VLAN tag being removed from Huawei hybrid switch port when changing data VLANs.
649974	FGT returning the wrong ARP value when multiple found.
650225	Aruba IAP SSIDs are not preserved when failed to read SSIDs
651375	Cisco WS-C3850 not correctly mapping as hybrid wired/wireless device. <b>Note:</b> This device model now appears in Topology as a wireless model since it can act as both a switch and wireless device.
651846	Clients not properly disconnecting and switching VLANs on Aruba Wired Switches using RADIUS Authentication. This is due to FNAC not including the User-Name in the disconnect request.
652156	FNAC not sending tag/group info via FSSO to FGT for non-root VDOMs.
652770	FNAC doesn't read sessions properly on some legacy Aruba WLC devices.
654510	The Remove Host and Adapters button doesn't work in the Locate View
655310	Administration UI produces 500 errors within advanced scan controls when attempting to manipulate security actions
655485	When Self Registration without a sponsor is configured to notify via SMS, the message includes "Sponsor: null"

Ticket #	Description (8.7.5.1519)
655609	Fixed Qualys vulnerability scanner integration
655820	Need to include latest agent
656180	Device Profiling fails to match DHCP vendor class
656980	FortiNAC is not sending FSSO tags to the FortiGate
656981	Read Only admin can enable/disable an adapter
657839	Error generated when synchronizing Control Manager (NCM) with PODs if a device profiler rule is configured for "Register as a Device in Host View and Topology"
657943	Upgrading to JSch 1.55 broke Cisco Sx300 SSH
658621	Radius Acct Stop handling thread (RadiusDisconnectThread) exits unexpectedly
623528 623534	Brocade type 7(MOVE) trap is processed incorrectly & showArp table parsing issue
655820	Includes agent 5.2.4. See agent release notes for details.

## Version 8.7.4.1517

Ticket #	Description (8.7.4.1517)
638344	Fixed firewall session polling. Previously, it was generating a null pointer exception in the master logs.
585370	Added RADIUS authentication support for HP ProCurve J4904A Switch 2848
601981	The SSID vlan customization for FortiWLC/Meru devices is showing the VLAN name and not the VLAN ID as it should be.
637391	FortinetEMSServerNullPointerException logged when authentication fails.
637327	Removed check for FortiAnalyzer serial number
637280	Added code to fix Device Profiling Rule rankings if corrupted
636385	Fixed Supplicant EasyConnect for Windows, macOS. It could not successfully create profiles or connect to the desired SSID.
631121	Added Wired RADIUS integration with Aruba/HP 2900 series
612477	Changed the default value for "Collect Application Inventory" to false for new Endpoint Compliance Configurations.
629260	Fixed communication issues between the NCM and pods

Ticket #	Description (8.7.4.1517)
635431	NCM Host view doesn't load properly for a pod in High Availability that has failed over.
606177 635285	JAVA use 100% CPU and high memory
633909	Updated "bscftp" alias to connect to the correct location.
631627	Fixed adding or modifying the Firewall Tag using the direct configuration. Previously, this would result in "HTTP 404 Not Found" error.
631249	Fixed incorrect modification of property file by .masterPropertyFile.
633364	Fixed Device Profiler DHCP method where attempting to match hostnames with 'D*' was matching with letter contained in any position.
633491	Fixed Error when saving a TLS Service Configuration with "Automatically Update Ciphers And Protocols on Upgrade" set. The modify dialog would not open until after FortiNAC was restarted.
632387	Fixed NMAP Scan Results Shows Wrong IP Address
632457	Fixed Run Nmap scan dialog title does not update with the current IP
621277	Fixed "User does not have permission for this operation" error when attempting to Set Expiration on multiple users.
622827	Cisco devices with no defined VLANs failed to read L2 data with SNMP  Fixed L2 polling not returning L2 information after upgrading Aruba controllers to ArubaOS 8.6.
636170	Fixed issue where registration can fail with multiple adapters (for example an Agent registration) when one adapter is invalid.

## Version 8.7.2.1513

Ticket #	Description (8.7.2.1513)
2969242	Location Based Policy Not Matching Due to SSID Name Containing ":"  Added FortiGate VPN Support
3491206 3809688	Added RADIUS authentication support for HP J9729A and HP J8697A
3817956	Fixed DNS behavior when system fails over in L3 High Availability configurations. Previously, the Secondary Server (in control) was replying to DNS inquiries with the Primary Server ETH1 IP address. This caused DNS resolution to fail for isolated hosts.
3571175 3624952	Fixed issue where FortiNAC could not L3 poll Fortigate FortiGate-201E

Ticket #	Description (8.7.2.1513)
3857250	
	Fixed FortiNAC Persistent Agent ADMX template value for disabling the Login Dialog.
3515941 3671084 3836414	Added client disconnect functionality support for WLC C9800
	Changes to support Swagger document generation
3730390	Fixed issue where the SSIDs tab would disappear
3629749	Added SNMP option for reading VLANs for Extreme devices. Enabling this option can improve VLAN read times on switches that support dot1qPvid.
3809105 3831066 3857251 3906623	Fixed Self-Registration accounts that do not require sponsor approval. Previously, this feature did not work after upgrading to 8.6.2 or higher.
	Additional clean ups and expansions to the REST API
3788773 3832801	Fixed connection issue between Control Manager and managed FortiNAC servers. Previously, this condition could cause the following behavior: <ul style="list-style-type: none"> <li>• Management processes on the Control Manager to report <code>down</code></li> <li>• Managed FortiNAC servers to stop processing RADIUS authentication packets</li> </ul>
	Fixed issue where exports of Device Profiling Rules to an XML file did not work
3787103	Fixed NCM Endpoint Compliance Policy Syncing issues
	AutoCompleteManager exceptions in catalina.out
	Fixed DeviceImport tool throwing "Unable to parse line" exception when a blank line is encountered in the CSV.
3815322	Fixed issue where Admin Profile Manage Hosts and Ports setting were not saved
	Fixed an issue where grab-log-snapshot did not gather the correct master_loader logs
3812378	Fixed alarms failing to trigger over time when any alarm was configured with an event frequency of "0" events occurring within X hours.
	Fixed issue where the enter key did not create an entry in the Add Logical Network dialog.
3817011	Fixed Log Receiver Syslog Facility not displaying in the Settings view.

Ticket #	Description (8.7.2.1513)
	Fixed issue where changing VLANs on newer Alcatel devices used the incorrect OID
	Added new methods to retrieve a HostRecord from an IP or MAC Address.
	Fixed issue where FortiNAC sent an incorrect serial number to FortiGate via CSF
	Fixed FortiNAC recognition time of when FortiGate connection is closed.
3801537	Fixed issue with high cpu/load averages on control server  Added <b>Rogue Evaluation Queue Size: NNN, Details</b> button and <b>Flush</b> button to the <b>Device Profiling Rules</b> view to provide better visibility and control over the rogue evaluation queue.
3816601	Fixed VLAN read/write on Juniper Ex 3400 switches.
3839246	Fixed <b>Apply to Group</b> drop down menu under <b>SSO Agent</b> options in the FortiGate model Elements tab. Previously, this menu was grayed out when the <b>Apply to Group</b> check box was selected.
3844800 3893874	Fixed issue with USB external adapter/dongle sharing between hosts. Agent technology can now be configured to remove adapters from the host record when the agent no longer detects the adapter connected. <b>Note:</b> This function is disabled by default and cannot be enabled through the Administration UI. Contact Support for assistance and reference KB article 193199.
	Fixed FortiGate modeling error with eight linked FortiSwitches
	Fixed an issue where Meraki SSID models are removed on a vlan poll when the SSIDs are disabled on the device
	Fixed restarting DHCP fingerprinting on ETH1 interfaces in HA environments
3836927 3873270 3873963 3896457 3952310 3964338 3978643	Fixed issue where Host IP address was not registered when connecting to FortiGate
3854444	Fixed processing of add/move/delete FGT syslog messages for managed FSWs in Link Mode.
	Fixed issue with attempting to access the REST API URL /api/server
3840671 4033732	Fixed Model Configuration not correctly mapping VLANs to individual switches

Ticket #	Description (8.7.2.1513)
3824602	Fixed issue with reading VLANs on Cisco 9000 IOS-XE
3872745	Modified Arista.mib login sequence
3872745	Support for Arista "switchport access" and "switchport trunk" modes
	Fixed Syslog parse error and null pointer exception with FGT Syslog connection updates
3879948	Fixed potential database corruption issue when using Device Profiling Rules with custom DHCP fingerprints.
3852483 3880329	Fixed issue where PODs were not synchronizing in NCM GUI
3813442 3931815	Fixed FortiSwitch ports disappearing after switch reboot
	Fixed issue where attempting to disable a host by IP Address using the REST API fails if the host is offline.
3860382 3879906 3924319 3926696	Fixed issue where uncompressed database backup replicated to secondary, causing 100% Disk usage
	Fixed issue where FortiNAC periodically did not gzip backup files on the Secondary HA Server.
	Fixed issue where FortiNAC replied with the wrong path to FortiGate via CSF
3896468	Added RADIUS Authentication support for Aruba JL256A and HP J9727A
	Fixed OutOfMemoryError when configuring Security Fabric settings
3979669	Added the ability for FortiNAC to be configured to respond to traffic using the same interface it was received (policy based routing). Required for VPN integrations and static IP environments. This function is disabled by default and requires configuration via CLI. Refer to the applicable VPN integration guide or contact Support for assistance.
	DHCP Fingerprint additions and updates
	Fixed issue where files in /var/named/chroot/etc are not replicated to the secondary
	Under <b>System Updates</b> , if the SFTP protocol is selected, an error dialog will display when attempting to save or test with any names where SFTP access is no longer supported to download code. Other names or IP addresses can still be configured to use SFTP.

Ticket #	Description (8.7.2.1513)
3952440	Fixed issue where FSSO Tag is added/removed constantly and toggles the applied firewall policy
3972339	For AWS, fixed ConfigWizard to display UUID and eth0 MAC address in license panel.
4024747	Fixed issue where the <b>Login</b> box of the Guest Self Registration page was greyed out, preventing registration after approval.
	Fixed potential issue in Device Profiler for rules containing an Active (AKA nmap) method.
	Fixed issue with Set Model Configuration View being non-functional.
3985152	Added support for new Checkpoints
	Fixed issue with Device Profile rules for Fortigate false positives matches
	Fixed potential NullPointerException error when "FortiGate" Method was used in Device Profiling Rule. This issue could cause the rule match to fail.
	Updated FortiNAC to support changes to the FortiOS firewall session table. Previously, FortiGate Session details were not displayed for when the FortiGate was running version 6.2.2 or newer.
	Fixed potential database corruption when using Device Profiling Rules after upgrade from 8.6 to 8.7
4018863	Fixed Adapter View not showing IP address of the host
	Fixed issue where the Maximum Concurrent License Count was incorrectly showing a small number greater than the licensed count (typically 4)

## 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

Ticket #	Description (8.7.1.1505)
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 <b>Settings &gt; Credential Configuration &gt; Persistent Agent &gt; RADIUS/LDAP</b> used Local instead of LDAP. Previously, the Persistent Agent did not register hosts when this option was selected.
	Added Security Actions to <b>System &gt; Groups &gt; In Use</b>
	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)
	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
2969968	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



Ticket #	Description (8.7.0.1503)
	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 8.7.6. These are in addition to the device support added in 8.6 and previous releases.

### Version 8.7.6.1523

Ticket #	Vendor
657680	Cisco C1111-8P
657680	C1111-4P routers
662090	Aruba WLC ArubaMM-HW-5K
663957	Alcatel R8 switches 6560(Vlan switching)
665441	HP FF 5700-48G-4XG-2QSFP+ Switch
665443	Cisco Catalyst 9606R
665445	Cisco Catalyst 9800-80 Wireless Controller
665448	HPE OfficeConnect switch 1820 24G J9980A

### Version 8.7.5.1519

Ticket #	Vendor
648463	Ruckus ICX7250-24-HPOE
648464	Palo Alto Networks Panorama server
648465	Dell Force10 S4048-ON series switch
648467	Cisco Catalyst C9404R
648484	Arista switch (DCS-7160-32CQ)
649227	Added support for new H3C Mac Notify trap
651337	Added RADIUS device support for Aruba JL258A 2930F
652378	Meraki AP models: MR36 Cloud Managed Indoor AP MR46 Cloud Managed Indoor AP MR56 Cloud Managed Indoor AP

Ticket #	Vendor
656976	MR76 Cloud Managed Indoor AP
	MR86 Cloud Managed Indoor AP
	Ruckus ICX7850-32Q
	Cisco IOS IE4000
	Arista Networks DCS-7050SX3-48YC8
	Ruckus ICX7850-32Q
	Aruba 9004
	OfficeConnect Managed Fast Ethernet PoE Switch

## Version 8.7.4.1517

Ticket #	Vendor
635714	Cisco 9200L IOS.XE 16.12
634583	Cisco IOS-XE 16.8 support
	Cisco IE20008TC (9.1.1472)
634251	FortiGate FWF60EV
636766	HPE 5130 24G 4SFP+ EI BR Switch (25506.11.1.208)
612667	XG210 Sophos firewall

## Version 8.7.2.1513

Ticket #	Vendor
3072972	Allied Telesis AT-GS924MX switch
3276178	
3842068	Arista Networks
3872745	
3527890	Aruba
3810253	Cisco
3874596	
3881725	
4002832	Added support for Cisco ASA Firepower models (ASA firmware required. Firepower firmware not supported): 2120

Ticket #	Vendor
	2130
	2140
	4110
	4120
	4140
	4150
	Extreme
3789334	FortiGate 6000F
3893941	FortiSwitch
	Hirschmann / Belden
3785857	HPE
3802588	HP
	Huawei
	ISW
	Meraki
3801248	NX5500 Wireless Controller

## Version 8.7.1.1505

Ticket #	Vendor
3531712	Cisco
3457026	
3620676	
3690680	
3431702	
	FortiSwitch
3746463	HP
3584288	Ubiquiti 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
	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 <b>Version_8_7</b> Systems running version 8.2.x and lower: Set to <b>Version_8_7_NS</b>
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© 2022 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.