FORTINAC RELEASE NOTES

Version 8.3.7
Release Date: June 24, 2019
Rev. B
July 1, 2019

Contents

FortiNAC Release Notes 1

Overview of Version 8.3.7 3

Supplemental Documentation 3

Version Information 3

Compatibility 4

Agents 4

Web Browsers for the Administration UI 4

Operating Systems Supported Without an Agent 5

New Features 6

Version 8.3.7 6

Version 8.3.6 6

Version 8.3.5 6

Enhancements/Addressed Issues 7

Version 8.3.7.860 7

Version 8.3.6.104 8

Version 8.3.5.13 10

Device Support 11

Upgrade Instructions and Considerations 12

Systems with Agents Running Pre-5.0 Versions 12

Upgrading from Pre-8.0 Versions with Agents Running 3.x Versions 12

System Update Settings 13

End of Support/End Of Life 14

End Of Support 14

End Of Life 15

Numbering Conventions 16

Overview of Version 8.3.7

Version 8.3 is the latest release being made available to customers to provide new functionality and address some known issues.

Important: If using agents, additional steps may be required after upgrade to ensure proper agent communication. See Upgrade Instructions and Considerations.

Supplemental Documentation

The following can be found in Fortinet Document Library
8.x Fixes and Enhancements Summary
FortiNAC Known Anomalies
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. For previous versions, refer to the Release Matrix document in the Resource Center on the Fortinet Networks web site.

Version: 8.3.7.860
Agent Version: 5.1.2.1

A newer Persistent Agent may be required to support certain antivirus and anti-spyware products. For the list of supported Anti-spy-ware and Antivirus software vendors log into the Resource Center and use the search options.

- 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	Internet Explorer version 9.0 or greater
Google Chrome version 26 or greater	Opera version 12.15 or greater
Mozilla Firefox version 20 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	Symbian
Web OS	Windows
Windows CE	Windows Phone
Windows RT	

New Features

Version 8.3.7

Description	Ticket #
None	

Version 8.3.6

Description	Ticket #
None	

Version 8.3.5

Description	Ticket #
None	

Enhancements/Addressed Issues

These changes have been made in FortiNAC Version 8.3.7.860. These Enhancements are in addition to the Enhancements that are outlined in previous releases.

Version 8.3.7.860

Description (8.3.7.860)	Ticket #
Active Active Ruckus SZ Configuration Resulting in Excessive Wireless Connections that fill up Connection Logs	3168631 3316197
Cisco 2821 router Layer 2 Support	3326191
If a subnet mask had a range including IP addresses whose last octet was "0", the rule would not match.	3337956
Sanitize Inputs for Pages that Provide Output from Inputs for CWE-79	
Add/Update DHCP Fingerprints	
Fixed the handling of Cisco MAC notification traps when configured for SNMPv3.	3309221
Issue updating host via API	3308700
Fixed Cajun/Avaya P-Series Switch support	3286861
Device Profiling rules with SNMPv3 methods not working	
Summit300-24 switch modeling issue	
Incorrect port format used for port substitution for CLI scripting on Cisco SG Switches.	3263916
Incorrect access provided to Admin Users with Helpdesk permissions (such as Network Devices).	2969466
Undo of Host Based CLI configurations did not allow a %port% substitution in scenarios when it should.	2969725
Changing the User Role to trigger a new Network Access Policy match does not result in an automatic VLAN Switch	
Switch Google+ Authentication to Google Sign-In for FortiNAC portal to accommodate the deprecation of the Google + sign in API	3182846 3220146 3222348
Under certain circumstances a network device could be created with a null type. This causes issues in the Topology view.	
Unable to change VLANs on certain firmware versions of Juniper EX switches due to incorrect mappings.	3228828
Unable to access MDM Services after upgrading to 8.3.6	3224382 3330904
Unable to login after renaming root account during initial setup.	3159200
NCM synchronization duplicating groups when pod was under heavy load.	3227120 3318294
When registering a host in the Portal the host role is incorrectly set to “BYOD”.	3217573

Description (8.3.7.860)	Ticket #
Added support for Cisco WLC CLI Login Sequence Changes in firmware version 8.8 and above.	3195219
Removed crystal reports from the product.	
FortiNAC is not sending data to Palo Alto	3120710
Fixed problem with profiling wireless hosts when location-based Device Profiling rules are used.	3189316
Fixed ability to read physical addresses of the FortiSwitch ports when being managed by FGT in FortiLink mode.	2969967
FortiNAC not responding to SNMP query	2997103 3039346 3097922 3171254 3325859 3341394

Version 8.3.6.104

Description (8.3.6.104)	Ticket #
Fixed L3 polling on Aruba controllers when the device returns entries without a mac address.	3159337
Added support for Juniper jnxL2aldMacChangedNotification trap.	3127458
Support added to FNC for hosts directly connected to FGT ports.	2969963 3107009
Support added for hosts managed on FGT devices.	2969185
Hosts Connected to FortiSwitches managed via FortiLink are not marked offline in a timely manner.	3035463
No Current or Default VLANs are populated on the FortiSwitch ports when performing a Read VLANs on the FortiGate.	3035463
Fixed visibility of ports in the Network Access/VLANs view for multiple FortiSwitches connected to a Fortigate in FortiLink mode.	3035463
Fix reading arp on Cisco using VRFs	3112984
Removed license restrictions to access REST API	3108386 3123681
Fixed results of "Test Connectivity" button in RADIUS server definitions on an FGT.	
Added DHCP Fingerprints for Windows 7, Windows 10, Linux/Raspian (AKA Raspberry Pi), Unix/Sun Ray, Printer/Canon, Printer/Dell, Printer/HP, Printer/Lexmark, Printer/Xerox, IP-Phone/Konftel, IP-Phone/Polycom, Gaming/XboxLive, Gaming/XboxOne	
Fix Aruba SSID deletion on startup when using VLAN mode.	2969921 3075760

Description (8.3.6.104)	Ticket #
After purchasing additional licenses, cannot upload .lic file using the License Management view of the Administration UI. The message "Invalid License Key" appears.	
Fixed issue where VLANs were not read correctly for Force 10 switches	
Users are unable to delete their devices using the Host Inventory.	3052871
Modified message for Verify Credentials to indicate that inability to contact the device is a possibility.	3024579
We now display an error dialog when Device Mappings fail to be reported. This dialog includes information to send manually to FortiNAC development.	
CLI credentials are checked successfully for FortiSwitches configured in Standalone mode.	
Fixed issue where SSIDs are removed from groups after FortiNAC loses contact with a FortiGate. This caused the SSID tab in the FortiGate Model to disappear.	
Added ability to assign IoT devices as identified by FortiNAC to specific FortiOS firewall policies.	

The following are resolved in both 8.3.6.104 and 8.2.14.52	Ticket #
Fixed handling of large SNMP GETBULK responses.	3094106
Lose search field in host view if a new filter in shared mode is created with "" or \	3154356
Improve Application Collection performance.	3146606
Added Global Model Configuration view for Aruba IAP devices	
Made Agent Communication status (lightning bolt icon in Host view) more reliable	3080081 3080632 3122780
Fix VLAN switching on certain Avaya VSP (Passport) switches and routers	3067239
Persistent Agent Cert Check CA uploads correctly, but is not read properly.	3130703 3168946
Add ability to change the VLAN via CLI for Ubiquiti Unifi switches	
Resolved issue communicating with older agents which could cause OutOfMemory in nessus loader after some time.	3072086 3123324 3146275 3210001
Fixed syncing of "Any/All" option in Endpoint Compliance Scans from NCM to pods.	3073422
Fixed handling of possible null value in a Pingable that could cause server startup to fail.	3058860

Version 8.3.5.13

Description (8.3.5.13)	Ticket #
Corrected mapping for Cisco s6t64 switch to reflect 6000 series device.	3039946
Fixed the problem affecting wireless connections to FortiWLC devices that do not appear connected immediately after authenticating.	3029092
Fixed problem with port group dialog not showing all the FortiSwitch ports on Fortigate devices.	
FortiGate not listing all sub switches in FortiLink mode in Topology View.	3017392 3035463
The following are resolved in both 8.2.13.12 and 8.3.5.13	**Ticket #**
Corrected mapping for Cisco s6t64 switch to reflect 6000 series device.	3039946
Fixed interface mapping issue on Dell R330 appliances.	3014190
Fix an issue where Dell devices with no enable password failed to log in.	3024617
Modified process for VLAN change on General Mode ports for Dell 7000 switches.	3028962
Changed the default API version for Ruckus SZ devices to v5_0	2969861
Change RuckusSZ to pull in APs by Name when available instead of Serial number	2969744
Hide ieee8023adLag (161) ports for Dell switches by default	
Users are now logged out of the Administrative user interface when user account changes from Administrative to non-Administrative, the password changes or the user account is deleted.	
Fixed situation where primary application server does not appear to sync properly after failover (L2 High Availability).	2968565
Fix an issue where certain Cisco devices running new IOS firmware fail L2 read via CLI.	
Fixed problem affecting wireless client disconnection when using Persistent Agent.	3008729
Fixed issue where large numbers of syslog parsing errors could cause FortiNAC processes to stop.	2992462
Fixed issue where adding a device with SNMPv2c specified adds it as an SNMPv1.	2981129

For a listing of fixes and enhancements for earlier 8.x versions, refer to the Fortinet Document Library.

Device Support

These changes have been made in FortiNAC Version 8.3.7. These are in addition to the device support added in 8.3.6 and previous releases.

Vendor	Ticket #
Adtran	
Airwatch	
Alcatel-Lucent	
Aruba	
Avaya	
Brocade	3298555
Cisco	3215154 3262903 3270414
Dell	3249910
D-Link	
ExtremeXOS	3242493
FortiGate	
FortWifi	
HP/Aruba	
HPE	
Huawei	3298555

Upgrade Instructions and Considerations

Important: Systems on version 7 *must* upgrade to 8.0 before upgrading to 8.1 or higher.

Systems with Agents Running Pre-5.0 Versions

For new installs and upgrades from older than 8.2, the "Default UDP" Persistent Agent Transport Configuration (UDP 4567) will initially be disabled. Agent versions 3.x and 4.x use both TCP 4568 and UDP 4567 to communicate.

Once upgraded to 8.3.1, re-enable the Default UDP Transport Configuration to allow FortiNAC to communicate to agents running pre-5.x versions.

1. In the Admin UI, navigate to **Settings > Persistent Agent > Transport Configuration**.
2. Under **Packet Transport Configurations** panel, click **Add**.
3. Fill in the fields with the values below:
   Name: Default UDP
   Bind to Address: (leave blank)
   Port: 4567
   Maximum Incoming Packets to Queue: 10000
   Transport Type: UDP
4. To apply changes, click **Reload Services**

Upgrading from Pre-8.0 Versions with Agents Running 3.x Versions

Upgrading FortiNAC from pre-8 versions to 8.x could break communication with agents running version 3.0 through 3.2. In agent versions 3.3 and greater, the communication protocol was changed from SSLv3 to TLS. This was done to address the POODLE vulnerability (CVE-2014-3566). As of Network Sentry 8.0.0, SSLv3 has been disabled completely.

Once upgraded to 8.3.1, re-enable SSLv3 until agents are upgraded.

1. Navigate to **Settings > Persistent Agent > Transport Configuration**
2. Under **TLS Service Configuration** panel, SSLv3 can be added in the **TLS Protocols** field.

Download FortiNAC Upgrade Instructions and Considerations from the Fortinet Document Library for information regarding upgrade instructions and additional considerations, including features no longer supported.

System Update Settings

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

Field	Definition
Host:	Set to updates.bradfordnetworks.com
Directory or Product Distribution Directory:	Systems running version 8.3.x: Set to **Version_8_3** Systems running version 8.2.x and lower: Set to **Version_8_3_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:** The use of SFTP has been deprecated. The option will be removed in a later release.

*downloads.bradfordnetworks.com will no longer be used as of January 31st, 2018.

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 8.1.0, Fortinet announced the End-Of-Life for FortiNAC 7.x. 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 firmware 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

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).