FortiNAC - Release Notes

Version 8.6.5

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

June 3, 2020
FortiNAC 8.6.5.1212 Release Notes
49-865-640148-20200603

TABLE OF CONTENTS

Overview of Version 8.6.5

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: 8.6.5.1212

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.

Note:

- Version 8.2.5 upgrade to 8.6.1
  - Not recommend upgrade
  - An upgrade to this version has to be for specific feature or function of the 8.6 release
  - Is generally available
  - Requires OS update to function properly
- Version 8.2.5 upgrade to 8.6.2
  - Requires OS update to function properly

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 8.6.5

There are no new features in 8.6.5.1212

New Features in 8.6.4

There are no new features in 8.6.4.1210

New Features in 8.6.3

There are no new features in 8.6.3.1206

New Features in 8.6.2

There are no new features in 8.6.2.

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 8.6.5. These enhancements are in addition to the enhancements that are outlined in 8.5 and previous releases.

Version 8.6.5.1212

Ticket #	Description (8.6.5.1212)
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
637280	Add code to fix Device Profiling Rule rankings if needed
636385	Fixed Supplicant EasyConnect for Windows, macOS. It could not successfully create profiles or connect to the desired SSID.
631121	Add Wired RADIUS integration with Aruba/HP 2900 series
629260	Fixed communication issues between the NCM and pods
631249	Fixed incorrect modification of property file by .masterPropertyFile.
632387	Fixed NMAP Scan Results Shows Wrong IP Address
632457	Fixed Run Nmap scan dialog title does not update with the current IP
636170	Fixed issue where registration can fail with multiple adapters (for example an Agent registration) when one adapter is invalid.

Version 8.6.4.1210

Ticket #	Description (8.6.4.1210)
2969242	Location Based Policy Not Matching Due to SSID Name Containing ":"
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.

Ticket #	Description (8.6.4.1210)
	Fixed FortiNAC Persistent Agent ADMX template value for disabling the Login Dialog.
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.
3788773 3832801	Fixed connection issue between Control Manager and managed FortiNAC servers. Previously, this condition could cause the following behavior: • Management processes on the Control Manager to report `down` • Managed FortiNAC servers to stop processing RADIUS authentication packets
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.
	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.
3817011	Fixed Log Receiver Syslog Facility not displaying in the Settings view.
3816601	Fixed VLAN read/write on Juniper Ex 3400 switches.
3839246	Fixed **Apply to Group** drop down menu under **SSO Agent** options in the FortiGate model Elements tab. Previously, this menu was grayed out when the **Apply to Group** 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. **Note**: This function is disabled by default and cannot be enabled through the Administration UI. Contact Support for assistance and reference KB article 193199.
	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

Ticket #	Description (8.6.4.1210)
3854444	Fixed processing of add/move/delete FGT syslog messages for managed FSWs in Link Mode.
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
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
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 bakcup files on the Secondary HA Server.
3896468	Added RADIUS Authentication support for Aruba JL256A and HP J9727A
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
	Under **System Updates**, 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.
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.
	Fixed potential issue in Device Profiler for rules containing an Active (AKA nmap) method.
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.

Ticket #	Description (8.6.4.1210)
	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

Version 8.6.3.1206

Ticket #	Description (8.6.3.1206)
3688356	Fixed HPE OfficeConnect 1950-48G VLAN change method
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.
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
	Changed **FortiGate** to **Firewall** under **Device Profiling > WMI > Windows Security Center**
	Fixed NullPointerException

Version 8.6.2.1203

Ticket #	Description (8.6.2.1203)
2969166	Fixed issue where users could not approve requests if user is in FortiNAC but not an Admin or a user in LDAP.
	Fixed exceptions in FirewallSessionManager
3500189	Fixed VLAN assignment behavior for RADIUS enabled wired ports when port and device are not in an enforcement groups.
	Added support for new FortiGate add/move/delete syslog messages for endpoints connection to FortiSwitch ports when in FortiLink mode.
	Fixed issue where the "Virtualized Devices" tab in Topology did not consistently display for Forti-products (e.g. FortiGate, etc).
3478803	Fixed issue where changing from SNMPv2 to SNMPv3 would still use SNMPv2.
	Fixed issue where FortiNAC was not finding the correct SSL port
3611173 3675268	Added support for obtaining L3 data from FortiSwitches operating in standalone mode.
3577488	Fixed incorrect substitution in /etc/hosts by the config wizard when the domain contained the string 'product'
	Updated UI and server so that Host Name and OS from the firewall are added to Rogue Hosts
3371004	Updated GUI for CDP set up and polling
	Added filters to API endpoints to filter on Fortigate sessions created since a timestamp.
3526064 3581484 3596866 3621688	Fixed issue where **Validate Credentials** in Topology did not test CLI credentials.
3658588	Fixed Network Device Summary Dashboard panel load performance
	Fixed NullPointerException
	Fixed issue where exporting host records did not display the correct name value used.
	Fixed issue parsing sessions from the FortiGate
	Configuration changes made to meet Samsung's unique captive network detection process
3555487	Fixed L3 polling problem with FortiGate devices.

Ticket #	Description (8.6.2.1203)
3526064	Fixed issue where Device Discovery saved bad CLI credentials although a valid user/pass was included in the test set.
3526064	Added filtering out known devices from Discovery Search
3440608 3448565 3458851 3464886 3466075 3466133 3473254	Fixed issue where ServerLimit value caused tomcat-portal to fail
	Add changes so that Device Discovery remains active when GUI Session Times Out
	Fixed Selecting & Deleting Fortigate Sessions
	Modified conditions of capturing open ports based on Active Device Profiling rules.
3535407	Fixed issue where **Search > Host View** did not actually complete search
3508168	Fixed potential ClassCastException when parsing Device Profiling Rules during startup
3547311 3629749 3634510 3665368	Fixed issue where Admin group members were deleted after a reboot or restart of services
	Added Logical Networks to **Group > In Use** checking
3537015 3663245	Fixed syncing Device Profiling Rule ranks.
	Fixed "SHOW WARNINGS" Database query behavior to improve performance
	Fixed Device Profiling Errors
	Fixed issue where **select > Edit** did not modify the selected record in **Access Configuration > Logical Network**.
2969932	Made changes so that keystrokes in the autocomplete fields of the Security Trigger now query a small subset of available autocomplete options using a fuzzy search, instead of preloading all available options and filtering on the client side.

Ticket #	Description (8.6.2.1203)
	Added version check to the install.bin OS updates for CentOS version 7.4 is required before installing FortiNAC 8.5+.
3584045 3612604	Add fixes to AP ownership of devices not configured
3532917 3552457	Made changes so that Upgrading to 8.6.0 or 8.6.1 with previously existing "Network Device Roles" will effectively disable it.
3548320	Fixed excessive DNS lookups in FortiNAC when using Aruba controllers
3686236	Fixed error with custom reports
3517564	Fixed the processing of SNMP link traps from FortiSwitches in FLink Mode when multiple FortiGate devices exist.
	Fixed initial setting of the alarms filter in the Dashboard Alarms panel.
3495438	Corrected Admin GUI description for **System > Settings > Persistent Agent**
3568191	Fixed process that was allocating more memory than necessary
	Added license information to grab-log-snapshot
	Fixed a delay before processes stop after issuing shutdownNAC / shutdownCampusMgr command.
	Added DHCP Fingerprints for various devices
	Fixed NumberFormatException while parsing IPv6 addresses
	Fixed issues where hosts managed by GSuite MDM service were not marked as managed by MDM
3090953 3504661	Added TRACE patch to files
3553430	Fixed issue where upgrading Cisco 800 to 15.9 IOS would render routers unable to poll devices.
3439028	Fixed reading VLANs on Juniper ex4600 switches.

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.

Ticket #	Description (8.6.1)
	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
	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	Fixed L2 polling for Aruba controllers running 8.5.x firmware.

Ticket #	Description (8.6.1)
3482984	
	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.

Ticket #	Description (8.6.0.320)
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 8.6.5. These are in addition to the device support added in 8.5 and previous releases.

Version 8.6.5.1212

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

Version 8.6.4.1210

Ticket #	Vendor
3072972 3276178	Allied Telesis AT-GS924MX switch
3842068 3872745	Arista Networks
3527890	Aruba
3822311 3810253 3874596 3881725 4002832	Cisco
4002832	Added support for Cisco ASA Firepower models (ASA firmware required. Firepower firmware not supported): 2120 2130 2140 4110 4120 4140

Ticket #	Vendor
	4150
	Dell
	Extreme
3789334	FortiGate 6000F
3893941	FortiSwitch
3785857	HPE
3802588	HP
	Huawei
	ISW
	Meraki
3801248	NX5500 Wireless Controller

Version 8.6.3

Ticket #	Vendor
3531712 3457026 3620676 3690680 3431702	Cisco
	Dell
3746463	HP
	Juniper

Version 8.6.2.1203

Ticket #	Vendor (8.6.2.1203)
	Alcatel
	Aruba
3550729 3556085	Cisco

Ticket #	Vendor (8.6.2.1203)
3437522 3411005 3515941 3671084	
	Dell
	DLink
	Extreme
	FortiGate 101E and 600E
	Foundry
	H3C
	HP
	HPE
	Juniper
	Linksys
	Meraki
	OAW-AP1221
	Ruggedcom Switch Line
	Smart Switch
	VSP

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).