FortiNAC - Release Notes

Version 8.5.2

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

July 29, 2019
FortiNAC 8.5.2.665 Release Notes
49-852-000000-20190729

TABLE OF CONTENTS

Overview of Version 8.5.2

Version 8.5 is the latest release being made available to customers to provide new 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 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.

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: 8.5.2.665

Agent Version: 5.1.2.1

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 8.5.2

Nozomi Networks Mobile Device Management (MDM) Integration

What it does:

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

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.**

New Features in 8.5.0

Logical Networks

What it Does:

Separates and decouples Network Access Policies from device specific network configuration values. Logical Networks are:

- Representations of network configurations that abstract access policies from the physical configurations.
- Used in the application of Network Access Policies and translate the logical access value to the physical values of network infrastructure devices. Thus decoupling policies from network configurations.

The configuration values are used by FortiNAC to provision the appropriate network access. One Logical Network can represent "N" physical network segments, simplifying the configuration of Network Access Policies.

Network infrastructure device specific configurations are done on the device or sets of devices associating the configuration values to the devices. This simplifies network access policy management by reducing the number of policies.

Security Fabric Connector Integration

What it Does:

- Enables FortiNAC to leverage user and host groups along with Firewall Tags in FortiGate policies.
- Enhances the FortiGate firewall integration to manage connections at Layer 3 through Layer 7 of the OSI Model.

How it Works:

Fortinet Security Fabric/FSSO Integration Guide

FortiGate and FortiWifi Connection Management Integration (Ticket 2969185)

What it Does:

Gives FortiNAC visibility and control over what is connected to the FortiGate. The connection can be direct wired connections or wireless connections through FortiWiFi.

How it Works:

FortiGate Endpoint Management Integration Guide

Mobile Deice Management (MDM) Integrations

Fortinet EMS Server (FortiClient)
Microsoft InTune
Google G-Suite API for Chrome OS device detection and registration

What it Does:

- Expands device Trust in FortiNAC to those devices managed by FortiClient EMS, Windows Intune and Google G Suite
- Further extends FortiNAC's endpoint visibility and trust of managed devices.

How it Works:

FortiClient EMS MDM Device Integration

Microsoft InTune MDM Device Integration

Google GSuite API MDM Device Integration

Device Profiling Methods WinRM Device and WMI

What it Does:

Provide enhanced profiling capabilities used to ensure the trust of devices Enhancing FortiNAC's ability to classify and trust devices and expand endpoint visibility

How it Works:

Device Profiler Configuration

FortiAnalyzer Integration

What it Does:

FortiNAC sends host information to the FortiAnalyzer for data logging and report generation.

Enhancements and Addressed Issues

These changes have been made in FortiNAC Version 8.5.2. These enhancements are in addition to the enhancements that are outlined in 8.5 and previous releases.

Version 8.5.2.665

Ticket #	Description (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
3175728	Fixed a bug where Extreme Switches were not clearing Current VLANs after a port is removed from the VLAN. Also now able to update Extreme Switches Current VLAN after being cleared.
3187751	Fixed hosts that register via Captive Portal losing Vendor Name
	Fixed Settings -> Syslog Files when licensed for FortiNAC Plus.
	Fixed problem with AP creation for Cisco WLC devices.
3354191	Fixed issue with Adtran VWLAN AP read where we'd fail to read the AP's IP Address.
3352649	FNC is now tolerant of Cisco WLC SSID/WLAN names containing trailing whitespace.

Version 8.5.1.613

Ticket #	Description (8.5.1.613)
	Security Risk Host and Host passed Security Test events not generated when Advanced Scans enabled
	dhcpd does not restart when configured for Access Point Management in 8.5.0.533
3326191	Cisco 2821 router Layer 2 Support
3309221	Fixed the handling of Cisco MAC notification traps when configured for SNMPv3.
3148572 3333489	Large 9.7GB dynamiclog.idb file in /var/lib/mysql/bsc/ on Primary Server. HA Replication Failing
3035463	No Current or Default VLANs populated on FortiSwitch Ports
3166840 3335535	Hosts are not allowed on the wireless network due to host's MAC being retained in DB while host record doesn't exist
3102103	IP set to = null port despite having an IP tied to an active interface
3093427	Registered/Authenticated Wireless hosts get network reconfig popups
3108462	Connecting VPN clients are not moved from isolation to production when Secondary Servers are in control
3320016	Remote FTP Server is invalid in remote back up config
3308700	Issue updating host via API
3243308	Multi-Access point alarm triggers with same MAC address
3041464	Discovery of large IP range can cause server to run out of memory
3337956	If a subnet mask had a range including IP addresses whose last octet was "0", the rule would not match.
	Juniper switch issue with reading default VLAN and changing port VLAN values
3338226	Microsoft InTune and FortiClient EMS MDM integrations not marking hosts as managed by MDM
	Summit300-24 switch modeling issue
3263916	The port format used for port substitution for CLI scripting on Cisco SG Switches is wrong

Ticket #	Description (8.5.1.613)
	Rogue DHCP Server Detection was broken by the recent security fixes
	Add/Update DHCP Fingerprints
	Device Profiling rules with SNMPv3 not working
	Network Access configuration and in Switch Model Configuration, only the first 25 are shown.
	DHCP Fingerprinting not running when the Control and Application Server are running on separate appliances.
3300672	Inconsistent results with location-based device profiling rules.

Version 8.5.0.533

Ticket #	Description (8.5.0.533)
	Access Policies added to Base
	License Added the ability to schedule a report that uses a Shared Host filter.
3113663	Fixed Self Registration Sponsor Login formatting that was missing.
	Fixed the error message pop up that appeared when changing your own password instead of redirecting back to the login screen.
	Added ability to perform NMAP type profiling scans without initially pinging the device.
	Added support for persisting open port information obtained from NMAP scans.
3087165	Improved performance of the process of disconnecting wireless clients.
	Added wildcard IP option for device profiling IP Range rules.
	Added support for Fortinet Security Fabric API.
	Removed the Crystal reports
2969725	Fixed an issue when undoing CLI commands where the %port% substitution would sometimes not work when it should.
3251540	User role changes now affect a re-checking of network access for each host registered to the user.
	Fixed FortiNAC GUI: navigating to Help > Customer Portal, the program now redirects to the Fortinet Support Portal.
3228828	Fix an issue with VLAN reads and VLAN changes for Juniper EX switches running certain firmware versions.

Ticket #	Description (8.5.0.533)
	Fixed an issue where under certain circumstances a network device could be created with a null type. This causes issues in the Topology view.
3227120	Fixed issue with NCM sync duplicating groups when pod was under heavy load.
3217573	The host role configured in the Captive Portal is ignored when hosts download the Persistent Agent and scan during registration. The role of "NAC-Default" is assigned instead. This appears to affect Windows machines with more than 2 adapters.
3195219	Support for new Cisco Wireless controller login sequence for version 8.8 and above.
3212126	Fixed Windows hosts with Persistent Agent not registering automatically by Device Profiling Rule. This was due to FortiNAC not waiting long enough for the Agent to communicate during evaluation.
3159200	Fixed ability to change the initial 'root' userID to something else during initial login.
	Added support for new Brocade MAC Notification trap OID (1.3.6.1.4.1.1991.0.201)
3120710	Fixed issue that prevented sending SSO data to PaloAlto.
3189316	Fixed problem with profiling wireless hosts when location-based policies are used.
3182846 3220146 3222348	Switched from using Google+ Authentication to Google Sign-In for FortiNAC portal.
2997103 3039346 3097922 3171254	Fixed support for SNMP queries to the FortiNAC SNMP agent.
	Added support for reading the list of device adapters provided by AirWatch API.
2969466	Changed the Host permission set to no longer grant access to view Port details without Network Device permissions. The functionality can be replicated by enabling Network Device Permissions with all associated views disabled.
3224382	Fixed bug preventing configuration of MDM Services.
	Added new "Connected Container" adapter field to the GUI.
	Added appliance platform support for Microsoft Azure and Amazon AWS.

Device Support

These changes have been made in FortiNAC Version 8.5.2. These are in addition to the device support added in 8.5 and previous releases.

Version 8.5.2.665

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

Version 8.5.1.613

Ticket #	Vendor (8.5.1.613)
	Alcatel-Lucent
	Aruba
	Avaya
3298555	Brocade
3286861	Cajun/Avaya
3270414	Cisco

Ticket #	Vendor (8.5.1.613)
	Dell
	FortiGate
	FortWifi
	HPE
3298555	Huawei

Version 8.5.0.533

Case #	Vendor (8.5.0.533)
	Adtran
	Aruba/HP
3262903 3215154	Cisco
3249910	Dell
	D-Link
3242493	Extreme
	FortiWifi
	HPE

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, 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.

Systems Configured for High Availability

Once upgrade is complete, re-save the High Availability configuration. This is required in order for the Primary Server to copy the license key to the Secondary Server. Otherwise, the function to fail over from Primary to Secondary Server will not work properly.

Note: Management processes are automatically restarted upon saving the configuration.

1. Navigate to **System > Settings > System Management > High Availability**
2. Click **Save Settings**

System Update Settings

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

Field	Definition
Host	Set to update.bradfordnetworks.com[1]
Directory or Product Distribution Directory	Systems running version 8.3.x: Set to **Version_8_5** Systems running version 8.2.x and lower: Set to **Version_8_5_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.

[1] downloads.bradfordnetworks.com will no longer be used as of January 31, 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 8.5.0, 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).