# FortiNAC - Release Notes

Version 9.1.0.0111

**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO LIBRARY**
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

**FORTINET TRAINING INSTITUTE**
https://training.fortinet.com

**FORTIGUARD LABS**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

February 25, 2021
FortiNAC 9.1.0.0111 Release Notes
49-910-699892-20210225

# TABLE OF CONTENTS

# Overview of Version 9.1.0.0111

Version 9.1.0.0111 is the latest release being made available to customers to provide functionality and address some known issues.

## Important

- 9.1.0+ uses a new GUI format. FortiNAC cannot go backwards to a previous version. Snapshots should always be taken on virtual appliances prior to upgrade.
- 8.8.x: When upgrading from a pre-8.8 version to 8.8 or higher, the upgrade may hang if the appliance does not have external FTP access. The upgrade introduces a new local RADIUS server feature that requires additional CenOS patches. The download and installation of the patches occur during the upgrade process. A new .repo file is written in order to download the patches and specifies FTP as the transfer protocol.
  Customers that currently do not have a README and want to upgrade themselves should do the following:
  **a.** Modify firewall to allow FTP access for the eth0 IP address for each appliance until upgrade is completed
  **b.** Once completed, modify the repo files to the desired protocol for future OS updates. For instructions, see section "Change Transfer Protocol to HTTP/HTTPS" in the CentOS Updates document in the Fortinet Document Library.
  Customers that currently have a README, do not want to upgrade themselves, or cannot make the temporary firewall change should contact Support to schedule the upgrade.
- Requires access to downloads.bradfordnetworks.com from each appliance or virtual machine. The update automatically installs CentOS files for the new Local Radius Server feature on the Control Server(s). If access is blocked, the software upgrade will fail. The default transfer protocol can be changed from FTP to either HTTPS or HTTP. For instructions, refer to the Appendix of the CentOS Updates (https://docs.fortinet.com/document/fortinac/8.3.0/updating-centos) reference manual.
- 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:** 9.1.0.0111

**Agent Version:** 5.2.6

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: 7.2 F 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 9.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



## New Features in 9.1.0

- New GUI Format
- Added ability to customize SMS and e-mail message client receives during Self Registration. For detail, see Send SMS messages in the Administration Guide.
- Added support for multiple VDOMs for WLC
- Detection of:
  - WIRELESS connectivity to non-whitelisted SSIDs (hotspot)
  - Dual-homed connections
- FortiNAC Portal Theme updated to look more modern
- Added MDM polling to the NCM level
- Captive Portal enhancements and Social Media Login options. See Social Media for Captive Portal in the Administration Guide for more details.

# Enhancements and Addressed Issues

These changes have been made in FortiNAC Version 9.1.0. These are in addition to the device support added in previous releases.

## Version 9.1.0

| Ticket # | Description (9.1.0) |
|---|---|
| | New GUI Format |
| 662191 | Added ability to customize SMS and e-mail message client receives during Self Registration. See Send SMS messages in the Administration Guide for more details. |
| 632115 | L3 Polling when FNAC enforces a VLAN change to any client. |
| 643102 | Sponsor input type using LDAP Group shows members of group twice |
| 648169 | REST API improvements related to the following:<br>• If no rank is specified when creating new role object, it will be created and placed at the bottom of the rank list for evaluation.<br>• Ability to create a new device type using one of the images available in the image archive on the appliance.<br>• Adding group members by type<br>• Improved internal handling when adding new groups |
| 653147 | Improved lookups for Plus and Base subscription license levels. |
| 655545 | FNAC VMs are missing FreeRadius/winbind packages |
| 662036 | FortiNAC does not support SSH to devices configured with DH group-18 |
| 670023 | GSuite integration uses cached user ID instead of the value entered in the UI |
| 677062 | Self Registration Login fails with "Multiple sponsors provided. None are valid." |
| 680495 | With None or Email selected for approval, no sponsor was associated with the Account Request |
| 693091 | Upload Image is blurry in Portal Configuration |
| 693247 | Local RADIUS loses NAS shared secrets on startup |
| 693520 | FortiGate VPN ports were not shown in inventory and VPN session initiation is slow. |
| 696668 | Admin UI should direct users to the config wizard when the appliance is |

| Ticket # | Description (9.1.0) |
|---|---|
| | unlicensed |
| 697305 | Proxy Radius throws exception when trying to log empty vendor-specific-attribute (VSA). |
| 697636 | logrotate permissions errors when run from cron for winbind and hotstandby logs |
| 697984 | When a VPN host is deleted from FNAC, the internal entry for it is not being removed. |
| 698066 | We fail to retry properly when the auth token expries for InTune API |
| 592831<br>671272 | Add an option to run an action on alarm clear. Also limit clear events to applicable events. |
| 626004 | Palo Alto Security Event Parser severity field value does not match Palo Alto event field value |
| 664989 | Admin user unable to enable host with access/modify/delete permissions |
| 670356 | Update GUI references from "Citrix Xenmobile" to "Citrix Endpoint Management" |
| 694398 | Vendor OUI database is not updating after auto-definition updates complete. |
| 695021 | SSO notifications for user logon/logoff to unknown location clients aren not processed. |
| 696939 | Changed mapping to support HPE1950 hybrid ports |
| 698344 | Corrected format for the default sponsor email in the tool tip. |
| 699103 | Firewall Polling should be Firewall Session Polling |
| 699919 | High Availability:database stops replicating and no error is reported |
| 699942 | The GroupModifyDialog doesnt always pull new data and is causing inconsistencies due to cached results |
| 700035 | dumpports cli tool exposes radius secrets |
| 700216 | Update VLANs can sometimes take a long time |
| 700574 | Event to alarm mapping window checkbox and combos are not working correctly |
| 701045 | Model configuration view missing components for several Cisco WLC devices |
| 701069 | Cannot filter on "Date Added" in Firewall Sessions view |
| 701399 | Fortinet EMS endpoint paging not working correctly |
| | Wrong column checked in trigger for TLSServiceConfiguration update |

# Device Support

These changes have been made in FortiNAC Version 9.1.0. These are in addition to the device support added in 8.7 and previous releases.

## Version 9.1.0

| Ticket # | Vendor (9.1.0) |
|---|---|
| 612738 | Nokia DSLAM Switch 7360 ISAM FX Switches |
| 673023 | Huawei S6720-26Q-SI-24S-A |
| 680809 | Dell EMC Networking S3124<br>Dell EMC Networking N1108P-ON<br>Ruckus Wireless Inc (C) 2006<br>SG350-52 52-Port Gigabit Managed Switch<br>Cisco Sx220 Series Switch<br>Dell EMC Networking N3024ET-ON<br>Cisco IOS Software, C880<br>Meraki MS355-24X Cloud Managed Switch<br>Cisco Adaptive Security Appliance Version 9.12(3)12<br>SG250-08HP 8-Port Gigabit PoE Smart Switch |
| 695460 | Cisco NX-OS(tm) n9000<br>ProCurve 516733-B21 6120XG Blade Switch<br>CBS350-8FP-E-2G 8-Port Gigabit PoE Managed Switch<br>SF250-24 24-Port 10/100 Smart Switch<br>SG250-26P 26-Port Gigabit PoE Smart Switch<br>Ruckus Stacking System ICX7650-48Z-HPOE<br>24-port 10/100 Ethernet Switch<br>Arista Networks DCS-7260CX3-64<br>Arista Networks DCS-7280SR-48C6<br>SG200-26FP 26-Port Gigabit PoE Smart Switch<br>SG200-18 18-Port Gigabit Smart Switch<br>Arista Networks CCS-758-CH<br>Ruckus ICX7150-C08PT<br>Cisco IOS Software, C1700<br>H3C Comware Platform Software |
| 669219 | Viptela SD-WAN |

# System Update Settings

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

| Field | Definition |
|---|---|
| Host | Set to fnac-updates.fortinet.net |
| Directory or Product Distribution Directory | Systems running version 8.3.x and higher: Set to **Version_9_1** |
| 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)<br>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.

#### 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).