

A decorative pattern of concentric hexagons in a light blue color, arranged in a honeycomb-like structure, located at the top of the page.

FortiNAC - Release Notes

Version 9.1.6

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

January 27, 2023

FortiNAC 9.1.6 Release Notes

49-915-769105-20211216

TABLE OF CONTENTS

Overview of Version 9.1.6	4
Important	4
Supplemental Documentation	5
Version Information	5
Compatibility	6
Agents	6
Web Browsers for the Administration UI	6
Operating Systems Supported Without an Agent	7
New Features	8
New Features in 9.1.6	8
New Features in 9.1.5	8
New Features in 9.1.4	8
New Features in 9.1.3	8
New Features in 9.1.2	8
New Features in 9.1.0	9
Enhancements and Addressed Issues	10
Version 9.1.6	10
Version 9.1.5	13
Version 9.1.4	16
Version 9.1.3	18
Version 9.1.2	22
Version 9.1.0	29
Known issues Version 9.1.6	32
Device Support Considerations	36
Device Support	38
Version 9.1.6	38
Version 9.1.5	40
Version 9.1.4	40
Version 9.1.3	42
Version 9.1.2	43
Version 9.1.0	46
System Update Settings	47
End of Support/End of Life	48
End of Support	48
Agent	48
Software	48
Hardware	48
Appliance Operating System	48
End of Life	49
Software	49
Numbering Conventions	50

Overview of Version 9.1.6

Version 9.1.6 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 CentOS 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 various components of the product. The software version and Agent version supplied with this release are listed below.

Version: 9.1.6

Agent Version: [[[Undefined variable FortinetVariables.Agent Version]]]

A newer Persistent Agent may be required to support certain antivirus and anti-spyware products. Refer to the Agent Release Notes in the [Fortinet Document Library](#).

Firmware version represents a collection of system services and operating system features imaged on to the appliance before it leaves manufacturing. The firmware image cannot be updated by a Fortinet customer. Services within the image are updated by Fortinet or a certified Fortinet Partner in appliance maintenance packages released as new more robust and secure versions of services become available.

Note that upgrading software versions does not change firmware nor does it automatically require an upgrade to the Persistent Agent. Newer Persistent Agents are not compatible with older software versions unless that capability is specifically highlighted in the corresponding release notes.

Compatibility

FortiNAC Product releases are not backwards compatible. It is not possible to go from a newer release to any older release.

Example: 8.1.1.132 cannot be downgraded to any other release.

To backup the current system prior to upgrade on virtual machines, perform a snapshot. For physical appliances refer to the document [Back Up and Restore an Image of a FortiNAC Appliance](#).

Agents

FortiNAC Agent Package releases 5.x are compatible with FortiNAC Product release 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 9.1.6	8
New Features in 9.1.5	8
New Features in 9.1.4	8
New Features in 9.1.3	8
New Features in 9.1.2	8
New Features in 9.1.0	9

New Features in 9.1.6

There are no new features in 9.1.6.0162

New Features in 9.1.5

There are no new features in 9.1.5.0147.

New Features in 9.1.4

There are no new features in 9.1.4.0141.

New Features in 9.1.3

There are no new features in version 9.1.3.0134.

New Features in 9.1.2

- Added the ability to send FSSO information to the FortiGate even when the endpoint is not directly connected. Requires the Persistent Agent. For details, see section "Unknown Location Endpoint Management" of the FortiNAC Security Fabric Integration Guide in the Document Library.

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 9.1.6. These enhancements are in addition to the enhancements that are outlined in 8.7 and previous releases.

Version 9.1.6

Ticket #	Description (9.1.6.0162)
640841	SSH connection to some AlaxalA switches fail.
741373	Support for Mobile Iron V2 API
743180	Issue with parsing saved filters that are blank in SharedClient Filters.
746585	Cisco Mac Move Notification Trap support.
752792	Device Profiling Rule registration not setting user/group membership.
754605	Added Tripp Lite DHCP fingerprints
756499	Support for "ethernetMacAddress" for MicroSoft InTune MDM integration for the latest API.
757705	Legacy SSO requires tags to be configured even though they are not used.Applies to FortiGate integrations.
758009	Added support to change VLANs via CLI on Allied Telesyn 8000S.
759018	Admin user with admin user profile permissions to Access, Add/Modify and delete "Users" is unable to create a new regular user.
761276	User/Host Profile with Location does not use Portal defined in Portal Configuration.
762081	bsc-rename-ethers service fails on virtual machines.
762702	Improved FortiClient EMS polling.Previously, not all hosts were retrieved upon a poll, causing some hosts not to register.
765477	FortiClient EMS test connect still fails after correcting a credential mistake.
765483	Fortinet EMS Version parsing is broken for EMS 7.0.
766600	L3 polling support for Inhand IR915L Router
767209	Aerohive VLAN interfaces do not update on resynchronization after VLAN ID or Profile ID change.
768329	Fail to determine port type for Cisco SG Switches with latest Cisco firmware.
768785	The GUI value "Registered Host" now displays as "Registered Host With

Ticket #	Description (9.1.6.0162)
	Owner".
768822	FortiSwitch does not respond to Change of Auth (COA) packet due to FortiNAC not sending the correct secret.
769558	NullPointerException registering a rogue host from the Hosts View.
769851	Accounting Stop Message is discarded from Link Mode FortiSwitches when using Local Radius.
770034	FGT 1800F labeled as 1500D
770208	Juniper switches fail to change VLAN on ports that are RADIUS enabled.
770695	Local RADIUS fails to find correct port on Extreme Summit X, preventing proper VLAN assignment.
770738	Ruckus API version detection not working for login API
770930	High L3 Polling frequency in environments with no SSO management configured.
771038	Port State Actions without clear actions cannot be saved in Event to Alarm mapping.
771149	"Confirm Device Rule on Connect" does not work properly when "Confirm Device Rule on Interval" is also enabled within the same Device Profiling rule.
771157	MobileIron Cloud application poll can fail if licenseID is too long.
771506	Erroneous creation of redundant unique keys could overfill Group table key limits.
771685	Apresia integration RADIUS 802.1x support incomplete.
771705	Change Inhand mib file to not use WRITE_HIDDEN in 9.1. and 9.2.
773828	Not polling L2 information from PNetworks switches with latest firmware.
773841	Meraki Switch VLAN read/set fails when the ifIndex does not match the dot1d index.
774202	Adjusted timestamp in syslog CEF message format.Previous formatting prevented some systems from properly processing syslog from FortiNAC.
774724	Unable to filter Hosts and Adapters by status through API.
776123	Unable to add/modify groups starting with "!" (bang).
777124	A higher ranked policy more general than a lower ranked policy is still honored if disabled.Lower ranked policy displays with a strike-through and is ignored.
777511	RADIUS support for HP 2910 and 2920 switches.
777778	Juniper switch VLAN change fails using 802.1x authentication and Proxy

Ticket #	Description (9.1.6.0162)
	RADIUS.
778108	Windows domain check Device Profiling method fails if there is no domain user logged on.
778112	Performance issue when performing group membership lookups.Symptoms include usually high CPU utilization.
778157	L2 Polling issues with Cisco 9800 WLC firmware 17.3.
778520	Added SQL query for GroupManager.getGroupsMembershipIDs() when determining group membership in order to improve performance.
779901	Vulnerabilities in mysql versions less than 5.6.42.
780626	Huawei Wireless controller imports nameless APs.
780790	CLI Failing to Alcatel Omni 6860-P48.
782374	L2 polling not parsing correctly for Motorola 7.X devices.
782740	Unable to read default and current vlans for Ruijie switches.
783227	Operating System updates from the UI fail when freeradius gpg key is not present.
783544	Fortigate FG-200F improperly labeled as FG-201E.
783621	Host import related Memory issues.
783944	Exception reading VLANs or SSIDs on Meru 4100 with firmware 5.1-93.
784601	Group membership lookup causing high CPU utilization.
784957	Not polling L2 information from Cisco ME-3400E-24TS-M router.
786401	Remote Scan -> Linux x86_64 -> 500 Error
787563	NullPointerException (NPE) during L2 poll of Meraki.
787585	DHCP fingerprints are not matching DHCP message type.
788825	<p>DHCP fingerprint additions, changes or improvements.</p> <p>Added: "Camera","D-Link"; "Camera","TRENDnet"; "HVAC","Honeywell"</p> <p>Updated: "Mobile","Samsung SmartWatch"; "Gaming","Nintendo"; "Network","Router/Netgear"; "Network","Router/D-Link"; "Network","Router/Trendnet"</p> <p>Changed Device Type: "Network","Apple TV" -> "internet_tv","Apple TV"; "Network","Amazon Fire TV" -> "internet_tv","Amazon Fire TV"; "Network","Chromecast" -> "internet_tv","Chromecast"; "Network","DIRECTV" -> "internet_tv","DIRECTV"; "Network","DVR/TiVo" -> "internet_tv","DVR/TiVo";</p>

Ticket #	Description (9.1.6.0162)
	"Network", "Roku Media Player" -> "internet_tv", "Roku Media Player"
790403	ClassCastException in AirespaceSwitch during WAP read.
790747	FortiGate interface with VLANs does not show device connections to VLAN sub interfaces for device detection traps.
794362	System Update not reliably trusting fnac-updates.fortinet.net.
793920	Default Admin Profiles Have No Permissions
782760	Huawei S7706 switch does not correctly reflect the interface port number in Label column.
792522	Fix Database auth changes for initial install
797465	Nested group memberships not detected.
794362	System Update not reliably trusting fnac-updates.fortinet.net.
799842	Endpoint Compliance - Policies: Takes 30 seconds to create policy, exception occurs due to user clicking OK more than once.
756499	MS InTune MDM integration does not support latest API.
782433	Fix Integration for D-Link DGS-3130-30TS.
784618	RADIUS Failures after upgrading from 8.5 to 8.8 due to bad secret.
788729	Randomly RADIUS 802.1x proxy stops working.
790854	Failure to properly read Cisco trunk ports results in undesired VLAN switching.
791304	Admin Profile > Uncheck All removes General permissions.
791327	FortiNAC is changing WAP Uplink ports Current VLAN to match the Default VLAN.
791342	Manually Registered IP Phones get incorrect device type assigned.
798511	Upgrading from 0159 to 0160 results in error: Access denied for user nac@localhost (using password: NO).

Version 9.1.5

Ticket #	Description (9.1.5.0147)
566257	Huawei wireless controller integration
609121	Support reading new SSID table format for Aruba IAP.

Ticket #	Description (9.1.5.0147)
707136	Audit Log overlay uses the same filters as the parent datatable.
723743	Unable to change VLANs on Cisco 9500 switch with TwentyFiveGigEthernet ports.
740427	FortiNAC REST API: Added API call "/device/move" (move a Network Device from one container to other container).
741639	Parsing issue reading VLANs and L3 data of DellSwitchOS10 models
742523	LDAP server shows up as a rogue host icon in Topology/Inventory.
742889	Virtualized Devices UI/Tab should not show the internal dmngmt-vdom.
746629	Support for Aruba switch mac notification traps.
746729	Added support for MobileIron cloud solution.
747920	During Device Discovery, SNMP v2c is now used by default instead of v1.
749846	Evaluation Time and High Availability tooltips are undefined in the License Management view.
751181	Cisco SG/SF switches with the word "All" in the banner fail to log-in.
753384	FortiNAC REST API: Added an optional boolean for "add-to-parents" that determines if doing an add or replace. Previously, would remove existing group membership unless both existing parent group and new parent group IDs were specified.
753385	FortiNAC REST API: Add-members now able to add a group to another group of same type (Host, User or Port) using Group ID.
753662	Telnet/SSH timeouts can now be configured per device from the CLI or from the "Credentials" tab in the UI.
754212	Security events not always resolving IP to MAC, resulting in inconsistent security event generation.
754619	Hosts CSV files with rule names could not be cleanly imported.
757749	Added REST API support for Ruckus v6.0. Previously, wireless clients connected to Ruckus were inaccurately showing offline in FortiNAC.
758282	DeviceManager NullPointerException
758517	Creating Guest accounts in GUI adds start date in the incorrect format.
758535	Improved performance of CSV imports. Previously, import was very slow.
759181	Improved event storage management. Previously, databases had the potential to grow unusually large, causing issues with upgrades and database replication in High Availability environments.
759245	DHCP fingerprints: Updated Wii and added definitions for LG internet TV and PS5.

Ticket #	Description (9.1.5.0147)
759768	RADIUS disconnect not sent for Juniper wired switches when using RADIUS authentication.
760197	macOS Monterey hosts running the Dissolvable Agent are unable to obtain configuration from server.
760409	Cannot L2 poll Ruijie switches.
760424	Check for OS updates from the GUI is failing.
760596	API reporting wrong FortiNAC version in its system/local-properties/cluster GET.
761362	ForwardingInterface debug:Enhanced API related output for FortiGate and FortiSwitch integrations.
761623	Added option to find host by serial number in PA server if unable to find by MAC address.Addresses issue where MicroSoft InTune sometimes returns randomized WiFi MAC Address (which are ignored by FortiNAC).
762240	Duplicate Groups in FortiNAC causing SSO Tags to not be sent.
762421	Proxy RADIUS to Cisco switch fails due to port lookup failure.
762438	EMS server integration failing to correctly report compliance.
762456	FortiNAC attempts to Deauth hosts that are not managed by FortiNAC from Aruba Controller SSID.
762743	Accounting Stop Message Discarded from Link Mode FortiSwitches.This prevents hosts from being marked "offline" as expected.
764011	Control Manager (NCM) Server List sometimes takes a long time to load.
765227	Roles on Manager (NCM) cannot be changed.
765252	Exception in CheckMacRunnable after initializing database.
765411	Not able to change VLAN's on Cisco Meraki MS250-48FP.
765562	Resynchronization of SSO sessions does not re-add any missing SSO sessions.
766595	NoSuchProviderException in Radius Certificate initialization logic.
768711	Cannot import host record CSV due to serialization error.
764017	New DHCP fingerprint definitions forFortiFone and FortiCamera (Operating System).

Version 9.1.4

Ticket #	Description (9.1.4.0142)
611613	Topology > Set Model Configuration option does not apply selected "Send Groups to the Firewall" and "Selected Groups" options for the FortiGate Virtual Device Model Configuration
666285	FGT interface with VLANs does not show device connections to VLAN sub interfaces
691918	Improved Local RADIUS/winbind service operation visibility and debugging in GUI
709559	Mist AP L2 Polling failure
721204	D-Link Switch Mac Notification trap support
728862	Enhanced DeviceImport CLI tool including SNMPv3 support. For details on all options, type "DeviceImport" in the CLI
734133	Pnetworks switch integration
735553	CLI and Vlan switching not functioning for Allied and Rugged devices
735791	Secondary servers do not retain contract entitlements
739674	Local RADIUS post-auth failing - Null Pointer Exception attempting to auth on generic/unknown devices (Moxa)
740229	Control Manager (NCM): Renaming scans and syncing creates duplicate scans
741811	Update of Adapter IPs causes empty replaces of DYNAMIC table
741864	Switching port vlans fails for Rugged devices
741929	Control Manager (NCM) is throwing an IOException for Too many open files
741938	HostRecords are cached by mac & used by multiple processes which can overwrite PolicyHints field in use by different process
741952	No response when adding new network devices
742347	IndexOutOfBoundsException in BridgeManager.VlanVerifyVector.put()
743243	Remove unnecessary exceptions for Jamf JSON parsing
743543	Caching of dot1qIDtoVIDMappings not working on Juniper switches
743627	RADIUS CoA not working with Ruckus mac-authentication sessions
744025	Location based Device profiling rule does not work consistently
744100	Unable to pull mac address information from Ruckus running V 5.2.Ruckus requires REST queries to contain a serviceTicket
744313	SNMP errors for Mist APs in Event Logs

Ticket #	Description (9.1.4.0142)
744371	Request count is set to startIndex+999, rather than endIndex-startIndex
745058	Unexpected duplicate and invalid mac addresses in Airwatch MDM cause slow or failed MDM polls
745083	Control Manager (NCM) Sync fails with ArrayIndexOutOfBoundsException
745133	SSH is intermittently failing to some Cisco devices
745444	Certificate Upload and Delete not working for RADIUS targets
746551	TAG not assigned in VDOM other than root
746570	Importing using Start Discovery errors with start IP must be after end IP
746923	Server startup may hang if the appliance doesnt have access to the web
746958	Local RADIUS cant find root VDOM for wireless authentication
746959	nacprobe service does not restart after failure
746986	Separate app servers unable to update OS when using fnac-updates.fortinet.net
747265	Hosts learned from AirWatch with unusually long hostnames
747276	Mist APs created with incorrectly formatted MAC address, L2 polling doesn't work
747324	When using port security on this switch, FortiNAC can no longer see any MAC addresses connected and is unable to read anything
747378	Unable to register multiple hosts as a device from host view
747935	Local RADIUS - "Authentication Failure" event/alarm is triggered after successful authentication
748041	Default Portal Self-signed cert is owned by root, should be nac. Causes deployment of new self-signed certs to fail
748661	Not sending SSO tags for Fortinet VPN clients
749837	Potential ClassCastException syncing objects between Control Manager (NCM) and pods
750264	Network Inventory incorrect after moving FortiGate with managed AP's to another container
750287	Rebooting Ruckus SZ Controller causes SSID configurations to return to use Inherited
750513	SSO information is not sent in 3rd party SSO integrations
751158	Rename existing RADIUS attribute group throws sql exception, can no longer retrieve all groups
751194	When adding a new Security Fabric Service Connector did not default to port 8013 when it should

Ticket #	Description (9.1.4.0142)
751408	Local RADIUS should use VDOM for radius mode when SSID context exists but is set to inherit config from device
751753	Ports view blank for some FortiSwitches in Link mode.
751780	Error dialog is displayed when registering an adapter as a device in Topology
752512	Unable to Assign VLANs on Ruckus Using Local RADIUS
752785	Control Manager (NCM) Synchronization can produce Null Pointer Exceptions in the logs
752788	Alarm view fails to load due to Null Pointer Exception
752838	Profiled Devices edit Rule Settings unable to be disabled
752951	SNMP occasionally parsing MAC addresses incorrectly
753414	Roaming Guest configuration left off of Aruba model configuration
753566	Dropdowns in the VDOM Configuration view are bounded by the body of the dialog
753908	Unable to import/export Device Profiling rules via UI or REST interface
755323	Assigning VLAN ID to Dead End Vlan fails with UI error "Invalid ID - Dead VLAN"
756126	Unnecessary FortiGate related log messages printing by default.Moved these messages to debug level logging
741938 753267	Policy Details in GUI shows wrong results.

Version 9.1.3

Ticket #	Description (9.1.3.0134)
650216	Unable to set firewall tags for PaloAlto model
666660	If a shared filter contains an exclamation point (!), a delete or edit silently fails
676232	Host with a disabled logged on user is not moved to dead end
684657	Improved the communication method between Control Manager (NCM) and pods by using REST API and certificate client authentication over HTTP Requirements: <ul style="list-style-type: none"> Manager must be installed with License key containing certificates (not required for pods). For more information see related KB article FD52784

Ticket #	Description (9.1.3.0134)
	<ul style="list-style-type: none"> Firewalls allow TCP port 8443 between Manager and pods <p>If the above requirements are not met, the Manager will use original communication methods</p>
693625	REST API > Groups > Groups service does not check for usage across different configurations
700276	Added Contact Status Polling to Element tab for Link Mode FortiSwitches
705845	Searching groups by name in Roles and Network Device Roles views doesn't work
709965	Server List panel in Control Manager Dashboard takes several minutes to build
712678	Clicking on a user count in the User Summary Dashboard panel does not create a Filter when it opens Host View
712695	Could not log in with a password containing a plus (+) symbol
713181	Added Import button for uploading hosts from an external file
713259	Meraki Ports/Interface creation issue when the Group Policy name is assigned to Production Logical Networks
713505	Nokia switch port names do not contain switch name
723563	Event Alarm Mapping not adding host or event information to Email Action
724173	CoA not working on Fortigates with FortiLink switch, where secret is defined on the switch
724383	Intermittent failure polling clients connected to FortiSwitch in Link mode
724769	When choosing groups for a Role, the slide-in panel lists all groups instead of limiting to User and Host groups
725360	Fix potential ClassCastException in MibObject
725604	Hosts are automatically approved by the system when "Registrations Require Approval" is configured under "Standard User Registration Approval" in the Captive Portal
725746	Communication issues between Control Manager (NCM) and POD can cause Endpoint Compliance scan failures
725751	"Sync initiated" event added. Generated when a synchronization of servers by Control Manager has been triggered. Provides server IP, the user who triggered the sync and status.
725757	Scheduler Modify dialog, Next Scheduled Time validator doesn't accept new time format
725969	"System Error" balloon pop-up when creating roles
725972	Removed unnecessary startup RelationInterface message from

Ticket #	Description (9.1.3.0134)
	output.master
726099	FSSO processing performance enhancements
726410	When a FortiLink Switch is renamed, the device and port model names in FNAC are not updated
726458	DPC rule does not revalidate upon connect for RADIUS clients ("Confirm Device Rule on Connect")
726678	Added custom Network Devices Admin Profile permission set to view/hide the device model Credentials tab
727066	Error dialog when setting device mapping to Generic SNMP using set device mapping option
727336	When collecting ARP information from ArubaOS WLC, the user table that contains the correct ARP entries is not being queried
727710	On upgrade from 8.8 to 9.1 or higher, the error "com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: Unknown table 'bsc.DatabaseAuditView'" may appear in the logs
728409	Hosts and Adapters views only show 999 Entries. The REST API is returning just the count of records in the current page.
728677	Local RADIUS Server fails to disconnect clients from Ruckus Virtual SmartZone (SZ) controller due to missing RADIUS attributes
728719	Add Device Profile Rule > Vendor OUI > Clicking Vendor OUI link results in HTTP 500 Error
729007	NullPointerException during V3 device creation via API when no v1 community strings provided
729585	Cisco ASA VPN clients not moved to the unrestricted group due to multiple values returned when reading object-group
730236	Failure to read SSID on Ubiquiti causes all SSID models to be removed
730601	Changing Endpoint Compliance scan causes agents to be rescanned even when monitors were not changed
730789	When wired clients are authenticated by the Local RADIUS Server, the default VLAN is returned. Network Access Policy look-up is skipped
730823	Multiple calls to edit a User Host Profile via the API results in failure after the first attempt
730892	VPN solution L2 polling process excessively long.
730908	Errors with secrets with special characters like %
730990	UI rendering for Authentication Policies/Configs tied to wrong permissions
731215	Added support to read L3 tables on Dell OS10 switches with VRFs

Ticket #	Description (9.1.3.0134)
	configured
731633	SQL Exception is thrown during FortiNAC server startup
732229	Missing event and alarm definitions for ADMIN_PROFILE_MODIFICATION
732265	Aruba Controller model configuration view is not showing supported RADIUS controls
732340	dumpports does not show port IP address (requestString)
732580	Added "sar" output in grab-log-snapshot
732965	Local RADIUS Server functionality not working properly upon failover or recovery in High Availability configuration
733232	Unable to save private filters
733903	Setting Host Expiration field to "Never" resulted in inaccurate expiration dates (example 12/31/1969)
733969	Unable to poll Airwatch MDM hosts. Although MDM poll appears to complete, new registered hosts are not created
734792	API communication issues with FortiGate
734895	Unable to parse L2 table on Dell OS10 Switches
735444	All RuggedCom switch models are shown as RSG2300 in the Model Configuration views
735880	Versa switch property files not loaded correctly
736110	Excessive exceptions for DatabaseObjectAlreadyExistsException seen in logs
736465	MAC address label is hidden if the IP address field is disabled in the Game Register portal configuration
736501	Cisco ASA VPN users are not always unrestricted after connecting.
736553	Log format has changed to include the thread ID and to remove redundant timestamp in heartbeat messages
738093	ISO build missing bc package
738257	Improved user look-up method to handle the different userID formats when matching Network Access Policies based on user record criteria. Previously, this was seen to cause delays in responding to RADIUS Accepts in some environments.
738375	RADIUS processing performance issues when RadiusManager debug is enabled
738805	Unable to set SSH port on Device Credentials page. Effects customers upgraded to 9.1.2

Ticket #	Description (9.1.3.0134)
739465	Removed Local RADIUS requirement that request must contain Service-Type=10(Call-check)
739674	Local RADIUS MAB & CHAP fixes
740034	Exception in RadiusManager with logging enabled.
740677	Backport of Model generation depends on updated Object Model
733892 733914	LicenseTool APPLIANCE shows EFFECTIVE count/level/certs if both are requested.
707284	VLAN ID and VLAN Name drop-down menu contents are now sorted in the Model Configuration View
714641	fortiGuardCB error in Device Profiling Rules view
732965	Local RADIUS not working properly upon failover and resume in a High Availability configuration
735553	CLI and Vlan switching not functioning for Allied and Rugged devices
739131	Replaced mysql-connector
739380	AirWatch does not retrieve all MAC addresses for enrolled devices
739674	Local RADIUS not working properly for MAC-address-based authentication (MAB) with generic/unknown devices (Moxa)
740723	Devices with VDOMs that specify Local RADIUS server/secret and use the Management IP - on restart the NAS DB tbl entry is removed
740749	Local RADIUS can only handle secrets of 60 characters or less
740962	Events on the Control Manager (NCM) to indicate synchronization of servers started and completed successfully or if there is a failure
741811	Update of Adapter IPs causes empty replaces of DYNAMIC table
741994	SSIDs added to groups with wrong type when added via SSID -> Group Membership preventing policy engine match on the group
742260	NullPointerException in DeviceServer.getVoiceVlans()
742261	NullPointerException in ProbeTelnet.getProbeObjectsByInetAddress()

Version 9.1.2

Ticket #	Description (9.1.2.0128)
725629	Unable to properly manage Aruba 9012 WLC due to incorrect mapping
677981	VPN Host FSSO tags not re-evaluated when host is disabled

Ticket #	Description (9.1.2.0128)
704761	If the "Delete Hosts No Longer Managed By MDM" option is enabled, hosts that are managed by Jamf may be deleted incorrectly
518423	802.1x support for Aerohive SR2208P
522462	Trigger "System Created Uplink" Events for Learned and User created Uplinks
543215	The Native VLAN on Juniper EX switches is no longer used. Juniper does not use or recommend using native VLANs
594554	VLAN Switch Success Event and Alarm now contain the "from" and "to" VLAN information
607004	MAC spoofing events do not generate when two endpoints with the same MAC address reside on two different switches at the same time. For configuration instructions, refer to the Administration Guide.
611202	Added support to report the status of the connection to the FortiGate
624926	Select Form Fields layout are not consistent with other fields in the Captive Portal
640641	The Persistent Agent Summary dashboard panel does not display the correct number of agents in the MAC-OS-X column
642707	Model Configuration View not accepting VLAN names in the Quarantine field (only VLAN IDs)
659675	"Rogue Connected" and "Device Created" events now include location (switch/AP and port), IP address, and "Connected Container" information
665191	Unable to get list of Devices in a container when querying FortiNAC using REST API
671704	FortiGate VPN - Host is registered as a device with no "Registered To" information and with "NAC-Default" Role
671997	Juniper Flex-CLI needs to account for configure mode prompt
672391	Generate MAC Spoofing events when spoofing and spoofed machines are on the same switch. For configuration instructions, refer to the Administration Guide.
676196	Sorting by columns does not work in the Legal Documents view
677981	Improved multiple VDOM support for FortiGate VPN integrations. Previously, FortiNAC was unable to determine correct tags to apply to sessions
682525	Added support to register Microsoft Intune clients with wired-only interfaces. Requires the FortiNAC agent. For details, refer to the MDM Integration reference manual
682625	ISO install now uses serial console for logging of VM builds.

Ticket #	Description (9.1.2.0128)
684437	When validating credentials, SNMP V3 succeeds even if the encryption protocol is incorrect
685185	Support for duplicate userids in multiple AD servers
687183	NCM does not support RADIUS for admin user authentication
687874	Add build type field to version file, displayed version in GUI
689049	Unable to properly manage Dell Switch S4128T due to incorrect mapping
691918	Improved diagnostic tools in Administration UI for local radius/winbind services
693627	Generated REST API token is shown in logs
693628	Uploading a trusted certificate to the same target multiple times throws an exception
695021	Added the ability to send FSSO information to the FortiGate even when the endpoint is not directly connected. Requires the Persistent Agent. For details, see section "Unknown Location Endpoint Management" of the FortiNAC Security Fabric Integration Guide in the Document Library.
696231	UI:Upgraded to Neutrino 1.0 library
696833	FortiNAC integration with FortiEMS:wrong API version used
697296	The Custom Ignored Adapters List (/bsc/campusMgr/master_loader/vendorCodes/ignoredAdapters.txt) is now added to System Backup
697937	Monitors are removed when any adapter is not found in the database, which can happen with virtual adapters
697994	VLAN Interface type Ports are Disabled on non-FortiGate devices
698090	Fortigate L3 polls do not support reading IPv6 arp data
698298	AP discovery not working for Extreme/Motrola Wing controllers on 7.X firmware
698728	Telnet/SSH to a FortiGate fail when post-login-banner is enabled
699077	Device Profiler - OUI method should take precedence over all other methods in a DPC Rule
699140	Radius port lookup fails on Nokia switch (Group ID 637)
699153	DeviceImport tool does not set the CLI credentials correctly on the created model
699606	A warning message now appears when attempting to install a legacy (NetworkSentry) license key using either the Administration UI or Configuration Wizard
700035	Minor formatting issue in dumpports password masking

Ticket #	Description (9.1.2.0128)
700128	FortiGate model creation takes a long time.
700312	Vendor OUI update are in agent/templates repo
700577	DHCP rule re-validation not working
700580	When polling the Fortigate, if there are multiple ARP entries for the same MAC address, the newest entry may not be used
700580	Fortigate L3 Poller throws exceptions for static arp entries
700610	Kiosk Page is not loading
700973	FortiNAC changing native VLAN instead of access VLAN and disabling PoE on VLAN switch
700992	Only ASCII characters are supported in FSSO Groups and tags
701358	Attempting to disable a host in Host View without proper permissions locks table, stays grayed out
701378	All API requests to a FortiGate fail when the post-login-banner is enabled
701766	Nessus loader shutdown and was not restarted
701796	Extreme switches detected wrongly as stacked in certain circumstances
702091	PersistentAgent server is failing to add monitor failure results when the last interface in list from agent doesnt have an adapter in FortiNAC
702259	Hostname information collected from FortiGate firewall sessions is no longer used for updating rogue host records. The information was sometimes inaccurate
702584	Delay in Local RADIUS authentication of EAP-TLS hosts
702585	Local RADIUS TLS Config omits v1.1 and writes tls_min_version=1.2 in error
702597	Missing event def RADIUS_SERVICE_RESTARTED
702978	Security Fabric Service Connector loads wrong record on edit
702989	Mist Wireless AP Discovery does not remove rogue
703008	FortiNAC now skips processing EMS device records that are no longer managed by EMS ("is_managed" value set to false)
703033	Added ability to skip registering EMS devices to a user. For configuration instructions, refer to the EMS Integration reference manual
703342	Added Address and Address Group Objects for use in VDOMs
703771	High Availability view in Administration UI now populates with default values read from /bsc/campusMgr/bin/.networkConfig
704582	NCM Dashboard Server List link to pod is broken

Ticket #	Description (9.1.2.0128)
704591	Legacy Hosts view - Auth Type and EAP Type columns not human readable
704601	Potential server startup deadlock
704603	Micosoft InTune Azure authentication not working
704713	Proxy RADIUS not ignoring empty string for VDOM shared secret causing RADIUS authentication to fail
705017	Settings > System Communication > Incorrect help text for Message Templates
706684	Device Profiler unable to set IP range 10.0.*.1 - 10.0.*.254
706706	Inconsistent scanning with "Scan on Connect" when connecting via VPN
706757	When creating a Device Profiling Rule under the Adapter View, the "Add Device Profiling Rule" option does not default to the NAC-Default role
707107	Unable to save Device Profiling Rule with Network Traffic method
707166	When doing a quick search from Host View, if a host has multiple adapters that all match the search query, each Dynamic Client is displayed independently
707270	Cameras are not matching the device profiling rule for DHCP Fingerprint Type Camera
707291	Fixed CLI Credential timing issue during device modeling
707581	Configuring Monitors on a Scan may fail
707655	Under certain conditions, guest sponsors get multiple approval emails
707722	Added CLI Tool to read arp cache entries collected by FortiNAC.
708193	NumberFormatException and IndexOutOfBoundsException when deleting a Fortigate (especially with no dependent devices)
708194	Ruckus device integration throws exceptions when CLI credentials are missing
708197	NASClientManager.multiObjectRemoved throws ClassCastException
708247	UI:Fixed navigation list component with new themes in Neutrino 1.0
708342	Meraki MX "Validate Credentials" and "Test Device Mapping" not working
708670	Install.bin cleanup: Remove code that is no longer needed
708671	Resync interfaces scheduled task for modeled FortiGate causes FortiGate SSL VPN FSSO client logoff. Hibernate Exception when removing extended client attributes
709269	FortiGuard Device Profiling method is not available on the NCM

Ticket #	Description (9.1.2.0128)
709278	Secondary Server in High Availability responds to RADIUS after Primary Server resumes control
709294	When using macOS browser to add FortiAnalyzer as a log receiver in the Administration UI: - Default port is now set to 514 - Ability to populate the Security string has been removed as it is no longer used
709318	SSH Known host keys can now be removed on-demand from the Credentials tab or automatically whenever a device is removed
709319	VPN integration code sends a VLAN-Switch to the Persistent Agent to inform it that its at risk. This leads to problems with Scan On Connect and unnecessary agent reconnection
709320	Device SSH keys didnt match /etc/ssh/known_hosts
709363	OS updates may fail due to i686 dependencies
709544	Eclipse environment error with non-jar ivy artifacts
709561	Passive Agent Policy group pull down does not show any AD groups if one of the AD servers is not reachable
709828	FortiNAC is using a default SSL certificate when connecting to FortiAnalyzer
709842	Improved reporting of the FortiAnalyzer connection state in output.master
709861	Added support for new API introduced in FortiGate/FOS version 7.x
709866	Fingerprint information not removed from database when host record is deleted
709868	Not Updating Rogue Host Name from DHCP Fingerprint
710058	ISO install is failing
710576	Additional data needed for FortiNAC CTAP reports
710646	Device Profiler Windows Profile method not working in HTTPS mode due to Command Line Too Long error
710971	Update MacAddressTable command to get RADIUS working for Huawei switch
711025	Removing an MDM service connector while there is poll in progress does not remove it
711510	PortLinkType not updated after resync interfaces
711696	Failure to switch VLANs on Cisco SG200-50 switches
712375	User/host profile does not match policy if Adapter information is used
712591	Changed wording for password configuration pop-up box in High Availability configuration for clarification.

Ticket #	Description (9.1.2.0128)
712658	Network Inventory takes a long time to load
712887	Fixed issue that might cause Device Profiler custom rules to not match correctly
712889	Only primary interface is imported to FortiNAC when host has multiple adapters
712980	Fail to display interfaces on certain Extreme switch models due to unexpected port format
713591	NEC QX Switches are discovered as generic SNMP devices.
713629	System/Settings/System Communication/Email Settings > Test Email settings works but SendEmail tool doesnt
713870	Failing to read arp cache on H3C
713962	Added L3 Polling support for Versa router
714399	Unable to add Cisco switch to Topology due to a Null Pointer Exception during modeling
714692	Removed iOS and Android from the "Add Device Profiling Rule" view.
714702	Not reading L3 from all VDOMs on a FortiGate
714764	Added license key upload button in Configuration Wizard.
714768	Unable to properly manage Alcatel-Lucent Enterprise OS6860E-P24 due to incorrect mapping.
714808	Ruckus L2 poll does not work with Ruckus version 6.x due to API changes.
715251	When RadiusManager debug is enabled and an unknown RADIUS attribute is received, NullPointerException is printed and FortiNAC stops processing the request.
715418	Trap handler debug states incorrect method says it's calling linkDown when it's calling linkUp
716371	"IllegalArgumentException:Invalid IPv4 address" log messages.
716411	FSSO tags are not sent when host role changes.
716599	RADIUS packets are dropped at times of peak usage.
716897	System>Settings>Trap Mib Files throws exception and does not function
717813	FortiNAC sometimes uses shutdown / No shutdown port to disconnect wired RADIUS client instead of RADIUS CoA
718168	Added API call /api/v2/user/set-password with userID and password parameters to modify a local user's password
718402	UI:SvgIconInterface isn't being loaded properly during build

Ticket #	Description (9.1.2.0128)
718783	FortiGate VPN failed to register for syslog and failed to login correct user if connection was lost without notification.
718802	Unable to collect host/user information from 6.4.3 EMS server.
718831	InTune group add causes database issues
719360	Unable to upgrade appliance if a legacy license Key is installed without Hot-Standby-Capable (High Availability).
719780	Catch All rule name inDevice Profiler is no longer modifiable.
720071	9.1 Online Help Generates 404 Error
720129	Upgrade to 9.x fails with "Unsupported group policy type java.util.ArrayList"
720360	Added FirmwareVersion attribute on the Aerohive SR22XX/Unifi switch models for 802.1x RADIUS CoA functionality
720439	RadiusManager property included in "radiusManager.properties" file
720467	FortiClient EMS integration:Added support for the mac_list property in the API
720471	Added cyber-blue MAC address 00:1A:7D:DA:71:15 to IgnoredAdapters.txt (Custom Ignored Adapters List)
721009	L3 polling of Viptela devices not working properly due to a missing property.
721566	Custom Scans Registry-Keys view produces an error
723851	DHCP Fingerprint for Mac OSX Bug Sur missing
725009	Imported LDAP group does not map to Administrators
716411	Hosts at risk do not trigger network change with FortiGate VPN and FSSO
715316	device synchronization doesnt work properly with VDOMs.
717912	Group Membership performance is too slow to handle load from policy engine
715316	
721743	Solo Randomized WiFi adapters ignored by PA server, Agent-Local IPs being set on adapters.
715316	
	Potential NullPointerException when generating agent fingerprint event.

Version 9.1.0

Ticket #	Description (9.1.0)
	New GUI Format

Ticket #	Description (9.1.0)
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: <ul style="list-style-type: none"> • 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. • Ability to create a new device type using one of the images available in the image archive on the appliance. • Adding group members by type • 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 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 expires for InTune API
592831 671272	Add an option to run an action on alarm clear. Also limit clear events to applicable events.

Ticket #	Description (9.1.0)
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't 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 doesn't 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

Known issues Version 9.1.6

Ticket #	Description (9.1.6.0162)
874037	GUI > Users & Hosts > Host View > Quick Search - Unable to locate host by hyphen or no delimiter.
882265	FortiNAC is not sending the correct serial number field to FAZ.
780312	FortiNAC does not integrate with Azure Active Directory due to SAML connection requirements.
754346	Default filter used when selecting Port Changes for a specific device port does not work.
874812	Private VLAN switching is not working > Cisco switches.
641036	Multi-factor authentication (MFA) for the Administration GUI login is currently not supported.
878059	Using Location that specifies a device will not work if that device is a FortiLinked FortiSwitch
686910 714219	Control Manager (NCM) communication issues when the NAC systems are connected through the WAN. For details see related KB article https://community.fortinet.com/t5/FortiNAC/Technical-Note-NCM-communication-issues-with-systems-across-WAN/ta-p/192434 .
752538	When in the Users & Hosts > Applications view, selecting an application and clicking the Show Hosts option displays a page that does not provide accurately filtered results. Workaround: Navigate to Users & Hosts > Hosts and create a custom filter to list hosts associated to an application.
766850	Landing page defined by an Admin profile is not honored. User with that Admin Profile is presented with the FortiNAC Dashboard instead. Workaround: Manually browse to intended landing page.
770091	Port changes/VLAN assignments made using local RADIUS are not being logged as port changes.
769014	"Generate Password Error" is displayed when adding new Guest/Contractor account. For details and workaround see KB article https://community.fortinet.com/t5/FortiNAC/Technical-Tip-Generate-Password-Error-when-adding-new-Guest/ta-p/209272 .
733943	Using "Set Model Config" for multiple Meraki wired devices can change Serial number to all be the same. It is recommended that edits to the device model are done on an individual basis as opposed to in bulk. There is no current workaround.
760926	Removal/Addition of LDAP model can cause user attribute synchronization issues. For details and workaround see KB article https://community.fortinet.com/t5/FortiNAC/Technical-Tip-Removal-Addition-of-LDAP-model-can-cause-user/ta-p/209296 .
754346	Selecting Port Changes under the Ports tab of a specific device in Network > Inventory does not display expected results. For details and workaround, see KB article https://community.fortinet.com/t5/FortiNAC/Technical-Tip-Default-filter-for-Port-Changes-does-not-populate/ta-p/209297 .

Ticket #	Description (9.1.6.0162)
792968	Legacy View for Users & Hosts > Hosts does not display items in tables. Workaround: Enter "*" (asterisk) in search field.
791442	Able to delete a Portal Configuration which is in use by a Portal Policy. Removal is done without warning the user.
726333	Entitlements (such as concurrent licenses) for Subscription Licenses are not accurately reflected in the Administration UI License Management view and only show Base licenses. Workaround: Use the License Information panel in the Dashboard instead.
718864	FortiNAC does not send all required attributes in CoA packets sent to Ubiquiti when an online host record is deleted from the database.
710416	There can be a delay in updating IP addresses for isolated hosts in host and adapter view.
708936	FortiNAC will logoff SSO for sessions that remain connected to a managed FortiGate IPsec VPN tunnel after 12 hours.
708720	Policy evaluation may not be triggered after a host status update in Microsoft Intune. This can prevent the host from being moved to the proper network. For details and workaround see related KB article https://community.fortinet.com/t5/FortiNAC/Technical-Tip-Policy-evaluation-not-triggered-after-Microsoft/ta-p/203843 .
694407	Linux hosts running CrowdStrike Falcon sensor 6.11 and later are not being detected by the agent. This causes hosts running CrowdStrike Falcon to incorrectly fail scans. For details and workaround, see related KB article https://community.fortinet.com/t5/FortiNAC/Troubleshooting-Tip-Linux-hosts-running-CrowdStrike-Falcon/ta-p/202694 .
682438	Page Unresponsive' error when exporting hosts. For details and workaround see related KB article https://community.fortinet.com/t5/FortiNAC/Technical-Note-Page-Unresponsive-error-when-exporting-hosts/ta-p/193878 .
677628	Cisco WLC Port Channel not classified as Learned Uplink. For details and workaround see related KB article https://community.fortinet.com/t5/FortiNAC/Technical-Note-Cisco-WLC-Port-Channel-not-classified-as-Learned/ta-p/196208 .
675180	False positive Scan Results when there are no sub-settings selected in Operating System check.
674438	"Processes" Scan Type option is not available when creating custom scans for macOS systems.
646580	Restarting FortiNAC services can generate a large number of SSH sessions with ASA. For details, refer to related KB article https://community.fortinet.com/t5/FortiNAC/Technical-Note-Restarting-services-can-generate-large-number-of/ta-p/195876 .
631115	Only 50000 records display in Adapter and Host Views. Example: Adapters - Displayed: 50000 Total: 57500
610581	L3 eth1 sub-interfaces are not removed after re-configuring an appliance configured for L3 Network Type to L2.
609976	Cisco WLC 9800 Model Configuration tab does not include the drop down VLAN lists under

Ticket #	Description (9.1.6.0162)
	Access Value. For details and workaround see related KB article https://community.fortinet.com/t5/FortiNAC/Technical-Note-Cisco-WLC-9800-Model-Configuration-tab-does-not/ta-p/198790 .
609046	A port where the master Aruba Instant AP (IAP) with VIP is connected becomes a "learned uplink". This type of uplink is not dynamically undone / removed when the IAP (with the VIP) is disconnected from that port.
522468	Although there are fields to set the role or access value in the Authentication portal, these functions are currently not supported.
747921	Portal renaming does not rename the associated CSS files.
5889702	Analytics Agent continues to run after configuration is removed from the UI. For details and workaround, see related KB article https://community.fortinet.com/t5/FortiNAC/Technical-Tip-Manually-Remove-Analytics-Server/ta-p/208596 .
695435	FortiEDR is currently not supported. If required, contact sales or open a support ticket to submit a New Feature Request (NFR).
675180	False positive Scan Results when there are no sub-settings selected in Operating System check.
674438	"Processes" Scan Type option is not available when creating custom scans for macOS systems.
762704	After clicking the 'restart services' button when applying SSL certificates to the Admin UI Certificate Target, the prompt does not clear and there is no confirmation dialogue (even though it was successful). Clicking the 'restart services' button again generates an error.
770974	Event Lifetime alarm trigger rule is not being honored when configured.
	Not all models of all network devices can be configured to perform Physical MAC Address Filtering even though the Admin UI indicates that the configuration can be set. Resolution: Hosts can be disabled by implementing a Dead-end VLAN.
	For Portal v2 configurations, web pages that are stored in the site directory to be used for Scan Configurations will not be included when you do an Export of the Portal v2 configuration. Resolution: The files in the site directory are backed up with the Remote Backup feature, but otherwise keep a copy of these files in a safe place.
	Removing a device from the L2 Wired Devices or L2 Wireless Devices Group does not disable L2 (Hosts) Polling under the Polling tab in Topology.
	The "Set all hosts 'Risk State' to 'Safe'" button changes the status of all hosts marked At-Risk to Safe. However, the status of the individual scans for each host remain unchanged.
	In a Layer 3 High Availability (HA) environment, configWizard must have a DHCP scope defined. Running configWizard without a DHCP scope can cause a failover.
	On FortiNAC appliances with CentOS 7, duplicate log messages may appear in dhcpd.log for each sub interface (eth1, eth1:1, eth1:2, etc).
	System > Settings > Updates > Operating System will only record and display dates of OS

Ticket #	Description (9.1.6.0162)
	<p>updates that are completed through the Administrative UI. If Operating System updates are run via command line using the "yum" tool, the update is not recorded. Resolution: Execute Operating System Updates through the Administrative UI in order to maintain update history.</p> <p>Only English versions of AV/AS and their corresponding definitions are supported.</p>
	<p>Anti-Virus product Iolo technologies System Mechanic Professional is currently not supported.</p> <p>Sophos UTM is currently not supported.</p>

Device Support Considerations

Ticket #	Description
548902	Management of wired ports on Aerohive AP-150W controlled by AerohiveNG is currently unsupported.
606729	The feature "Palo Alto VPN Integration" is currently not supported. It has been determined not to be ready for customer production use for managing remote user VPN connections through Palo Alto firewall.
679230	Aruba 9012-US currently not supported. If required, contact sales or support to submit a New Feature Request (NFR).
711696	Cisco SG200 support is limited to visibility only. The switch does not provide the management capabilities required for control/enforcement.
829009	The Allowed VLAN list is not properly managed on Aruba CX switches. When FortiNAC performs a VLAN change, only the new VLAN is set. The previously configured Allowed VLAN is not removed. This causes the Allowed VLANs list to grow over time.
836831	Layer 2 polling HPE Walljacks fails if special characters are found in the devices mac-address table.
842181	FortiNAC does not support the custom RADIUS attribute Fortinet-Host-Port-AVPair action=bounce-port for Change of Authorization (CoA) with FortiSwitches.
843509	FortiNAC is unable to communicate with Dell x1026 switches.
846782	FortiNAC is unable to read roles and potentially other data from Aruba IAPs due to a # symbol automatically added to the wireless network name.
	At this time, integration with Juniper MAG6610 VPN Gateway is not supported. This includes Pulse Connect Secure ASA.
	At this time, integration with Cisco 1852i Controller is not supported due to the device's limited CLI and SNMP capability. For details, see related KB article 189545.
	At this time, Fortinet does not support wired port management for the Cisco 702W. The access point does not provide the management capabilities required.
	At this time, Fortinet is not able to support the Linksys LAPN600 Wireless-N600 Dual Band Access Point.
	Ports on Avaya Networks 4850GTS-PWR+ switches sometimes show "Not Connected" even though the port is active. This is due to multiple ports on the switch using the same MAC Address. This prevents NAC from correctly discerning which are "Connected" versus "Not Connected". There is no workaround.

Ticket #	Description
	Device models for Avaya 4800 switches (and potentially other related models) only support SSH. Device models for Avaya Ethernet Routing Switches only support Telnet. Contact Support if the alternate protocol is required.

Device Support

These changes have been made in FortiNAC Version 9.1.6. These are in addition to the device support added in 8.7 and previous releases.

Version 9.1.6

Ticket #	Vendor (9.1.6.0162)
765568	Huawei AR550E router/switch
769085	MICROSENS G6 Micro-Switch S5731-H48T4XC FW_WLC
770214	S5300-52C-PWR-EI S5731-S48P4X Alcatel-Lucent Enterprise OS6465T-P12 Alcatel-Lucent Enterprise OS6465-P12 FG_GRP9 brayhall-core-router Meraki MR20 Cloud Managed AP
771979	SG250-08 8-Port Gigabit Smart Switch S5700-10P-LI-AC DC FortiGate Cluster
774429	Cisco NX-OS(tm) nxos.7.0.3.I4.1.bin, Software (nxos), Version 7.0(3)I4(1) Dell Networking X1018P 1Gb PoE Switch SG350-28 28-Port Gigabit Managed Switch Ruijie 10G Ethernet Switch with PoE (S2910C-48GT2XS-HP-E)
777886	D-Link DGS-3130-30TS System - 24*10/100/1000M + 2*10GBase-T + 4*10G SFP+, 145.1.10.57 Fortigate Cisco IOS Software, CDB Software (CDB-UNIVERSALK9-M) Quidway S7706 Huawei Versatile Routing Platform Software Cisco IOS Software, C880 Software (C880VOICE-UNIVERSALK9-M) Fortinet Cisco IOS Software, ir800 Software (ir800-UNIVERSALK9-M)
781634	S5700-52P-LI-AC Huawei Versatile Routing Platform
783982	S5720-12TP-LI-AC

Ticket #	Vendor (9.1.6.0162)
	S5720-36PC-EI-AC S5720S-52P-SI-AC S5700-10P-PWR-LI-AC
786422	ArubaOS (MODEL: 565)
787686	S5735-L48T4S-A1 Huawei Versatile Routing Platform Software VRP (R) software CBS350-48P-4X 48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks CBS350-48P-4G 48-Port Gigabit PoE Managed Switch CBS350-8P-E-2G 8-Port Gigabit PoE Managed Switch CBS350-24T-4X 24-Port Gigabit Stackable Managed Switch with 10G Uplinks Linux Lethe 2.6.18-92cpx86_64 1 SMP Mon Oct 8 10:34:42 IDT 2018 x86_64 Juniper Networks, Inc. srx380-poe-ac internet router, kernel JUNOS 20.4R3-S1.3 S5735-L8P4S-A1 Huawei Versatile Routing Platform Software VRP (R) software Fortigate fwf51E Quidway S9712 Huawei Versatile Routing Platform Software VRP (R) Software Brocade Communications Systems, Inc. FastIron SX 1600 CCB 1st Sessions Court FS108F Meraki MR36H Cloud Managed AP
792686	Huawei AR129CGVW-L Huawei Versatile Routing Platform Software VRP (R) software Cisco NX-OS(tm) nxos.9.3.7.bin, Software (nxos) Juniper Networks, Inc. ex4400-24p Ethernet Switch, kernel JUNOS 21.1R1.11 Aruba R8N85A 6000 48G CL4 4SFP Swch PL.10.09.1000 Aruba Instant On 1930 8G 2SFP Switch JL680A, InstantOn_1930_1.0.5.0 (139) IE1000 Industrial Ethernet Switch, Version: 1.7.0#2018-05-02T18:19:37+00:00
796633	Fortigate Cisco IOS Software, C1000 Software (C1000-UNIVERSALK9-M), Version 15.2(7)E4 Aruba R8N87A 6000 24G CL4 4SFP Swch PL.10.08.1010 Meraki MS355-48X2 Cloud Managed Switch Dell EMC Networking OS10 Enterprise.S5224F-ON

Version 9.1.5

Ticket #	Vendor (9.1.5.0147)
760460	FortiSwitch Dell EMC Networking N1124T-ON Alcatel-Lucent Enterprise OS6560-P24X4 Alcatel-Lucent OS6450-U24 ExtremeXOS (X620-16x) ExtremeXOS (X450G2-24p-10G4) Aruba R0M68A 2930M-24SR-PoE-Class6 Switch Aruba JL727A 6200F 48G CL4 4SFP+370W Switch Aruba JL675A 6100 48G CL4 4SFP+ PLANET, IGS-10020HPT, IE L2+ Managed Switch
761980	Alcatel-Lucent Enterprise OS6860E-P48 Alcatel-Lucent Enterprise OS6560-24X4 Alcatel-Lucent Enterprise OS6560-P48Z16 Alcatel-Lucent Enterprise OS6560-P48X4 CHS_Fortigate_VM04
763316	VSP-4900-12MXU-12XE
765550	Alcatel-Lucent Enterprise OS6560-48X4 Enterasys Networks, Inc. A4H124-24 24-port 10/100 PoE Switch w/4 gigabit ports S5735-L48P4X-A1 Huawei Versatile Routing Platform Huawei AR550E Huawei Versatile Routing Platform
766493	Dell PowerConnect 5548P
767310	HP 1910-24 Switch Allied Telesis router/switch, AW+ v5.4.6-1.5

Version 9.1.4

Ticket #	Vendor (9.1.4.0142)
734133	Pnetworks switch
743833	Cisco NX-OS(tm) nxos.9.3.5.bin Cisco NX-OS(tm) nxos.7.0.3.17.9.bin
745113	Dell EMC Networking OS S5730-68C-PWR-SI-AC Huawei Versatile Routing Platform Software VRP

Ticket #	Vendor (9.1.4.0142)
	<p>S5730-48C-PWR-SI-ACHuawei Versatile Routing Platform Software VRP SX350X-52 52-Port 10GBase-T Stackable Managed Switch PLANET IGSW-24040T Managed Switch Cisco IOS Software, CSR1000V Software (X86_64_LINUX_IOSD-UNIVERSALK9-M) Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M) Dell EMC Networking N2224PX-ON, 6.6.1.1, Linux 4.4.170-b055baf1 Dell EMC Networking N3024EF-ON, 6.6.3.36, Linux 4.14.138, v1.0.5 Dell EMC Networking N2248PX-ON, 6.6.3.10, Linux 4.15.18-2ac8b3ec Dell EMC Networking N3248P-ON, 6.6.3.14, Linux 4.15.18-2ac8b3ec Dell EMC Networking N1108EP-ON, 6.6.3.10, Linux 4.14.138 FortiGate Aruba JL677A 6100 24G CL4 4SFP+ Swch PL.10.06.0001 Juniper Networks, Inc. ex3400-24t Ethernet Switch HPE 1950 48G 2SFP+ 2XGT Switch Meraki MR53E Cloud Managed AP Linux cep-gate 3.10.0-957.21.3cpx86_64 1 SMP Aruba JL659A 6300M 48SR5 CL6 PoE 4SFP56 Swch FL.10.08.0001</p>
749162	FortiSwitch-108F-POE
752957	<p>Aruba Instant On 1930 48G 4SFP/SFP+ Switch JL685A HPE 5510 24G PoE+ 4SFP+ HI 1-slot Switch JH147A WS6-DGS-1210-28/F1 6.10.007 Dell Networking N1524 Palo Alto Networks PA-3200 series firewall HP 1820-48G-PoE+ (370W) Switch J9984A Hirschmann MICE Switch Power Hirschmann Rail Switch Power Enhanced USIDC-FWL001 swich standalone NetVanta 1534P AOS-W (MODEL: OAW-4030)</p>
754988	<p>FSW_248E_POE FSW_148F FSW_148F_POE FSW_148F_FPOE FSW_124F FSW_108F FSW_108F_POE FSW_108F_FPOE</p>

Ticket #	Vendor (9.1.4.0142)
	FSW_1024E FSW_T1024E FSW_124F_POE FSW_124F_FPOE
756556	Enterasys Networks, Inc. Bonded SSA Chassis Rev 08.11.04.0005

Version 9.1.3

Ticket #	Vendor (9.1.3.0134)
688048	ApresiaNP2000-24T4X ApresiaNP2000-24T4X-PoE ApresiaNP2000-48T4X ApresiaNP2000-48T4X-PoE Apresia13200-28GT Apresia13200-52GT Apresia5428GT Apresia3424GT-SS ApresiaLightGM110GT-PoE ApresiaLightGM110GT-SS ApresiaLightGM118GT-SS ApresiaLightGM124GT-PoE ApresiaLightGM124GT-SS ApresiaLightGM152GT
730834	Foundry Networks FWSX424+2XG Ruckus Wireless, Inc. Stacking System ICX7550-24F Huawei S5720-52X-LI-AC HP Series Router A-MSR30-10 H3C Series Router MSR30-10 Alcatel-Lucent Enterprise OS6350-P24 Alcatel-Lucent Enterprise OS6350-48 LGS308P 8-Port Gigabit PoE+ Smart Switch HPE MSR3012 Meraki MR44 Cloud Managed AP Dell S4112T-ON Aruba JL676A 6100 48G 4SFP+ Aruba JL679A 6100 12G CL4 2SFP+ Dell S5048F-ON Brocade ICX7150-48-POE

Ticket #	Vendor (9.1.3.0134)
	Brocade ICX7150-48-POEF HPE OfficeConnect 1950-24G-2SFP+-2XGT Huawei S5735-S48P4X Cisco NX-OS(tm) n5000
735445	Huawei Quidway S3352P-EI Huawei Quidway S9306
689049	Dell Switch S4128T (DellSwitchOS10)

Version 9.1.2

Ticket #	Vendor (9.1.2.0128)
663957	Alcatel-Lucent Enterprise OS6560-P24Z8
701094	Arista switch models
705003	Extreme 210-Series 24GE PoE+, 2 1GbE SFP ports Dell EMC Networking N3224PX-ON Dell EMC Networking N3248PXE-ON SF350-24 24-Port 10/100 Managed Switch Huawei AR109GW-L Alcatel-Lucent Enterprise OS6860E-P24 Cisco Adaptive Security Appliance FortiGate 201E Cisco IOS Software, ir800 Software ArubaOS Aruba7008-US Cisco NX-OS(tm) nxos.7.0.3.I7.9.bin Powerconnect 8024F, 5.1.0.1, VxWorks 6.6 Device Description: Dell EMC Networking OS Meraki MS355-48X Cloud Managed Switch Cisco IOS IE4000 Cisco IOS C800 AP7632 ArubaOS 505H Cisco IOS Software [Gibraltar] Cisco IOS C9800-AP Cisco Controller
706225	Ruijie XS-S1960
707895	Cisco C899 4G LTE Router

Ticket #	Vendor (9.1.2.0128)
708234	HP 1910-8 Switch
708273	Alteon Application Switch 4408XL Avaya Networks Ethernet Routing Switch 5698TFD ERS-8806 ExtremeXOS X435-8P-4S
708309	Add support for multiple cisco models
709545	Gateway Copper Switch ArubaOS W-AP103
709844	HP VC Flex-10 Enet Module SG500X-24P 24-Port Gigabit with 4-Port 10-Gigabit PoE Stackable Managed Switch SG200-50FP 50-Port Gigabit PoE Smart Switch Xirrus XH2-240 WiFi Array Xirrus XD1-240 WiFi Array Cisco NX-OS Cisco IOS C1000
709863	GbE2c L2/L3 Ethernet Blade Switch for HP c-Class BladeSystem Cisco IOS Software, C1600 Software (AP1G2-K9W7-M)
712593	Huawei S2700-9TP-PWR-EI Meraki MS125-48FP Cloud Managed PoE Switch Huawei S5735-S48T4X Extreme Networks, Inc. A2H124-24P Cisco Controller ArubaOS W-AP103
713591	NEC QX Switches: QX-S1016GT-4G QX-S4108GT-4G QX-S4116GT-4G QX-S4124GT-4G QX-S4148GT-4G QX-S3408FT-2G QX-S3416FT-2G QX-S3424FT-4G QX-S3448FT-4G QX-S4009P QX-S4020P QX-S4028P QX-S4052P

Ticket #	Vendor (9.1.2.0128)
	QX-S3309TP QX-S3318TP QX-S3326TP QX-S3852TP
714422	Planet IGS-10020PT
720989	Cisco IOS Software, C1000 Software (C1000-UNIVERSALK9-M), Version 15.2(7)E2 Huawei S5735-L24P4S-A Huawei S5735-L48P4X-A SG350-28SFP 28-Port Gigabit SFP Managed Switch ExtremeXOS X440G2-24x-10G4 ExtremeXOS X440-24x-10G ExtremeXOS X440-L2-24t ExtremeXOS X440-24x ExtremeXOS X620-8t-2x Industrial 6-P GbE RJ45 + 2-P GbE SFP L2 Plus Managed UPoE Switch Dell EMC Networking N3132PX-ON Dell EMC Networking S3148P Dell EMC Networking OS10 Enterprise Dell EMC Networking OS10 Enterprise Dell EMC Networking OS10 Enterprise Dell EMC Networking OS10 Enterprise Dell Networking OS Series: PE-FN-410S-IOM Dell EMC Networking OS10 Enterprise Dell EMC Networking OS10 Enterprise Aruba JL660A 6300M 24SR5 CL6 PoE 4SFP56 Meraki MS390-24UX L3 Stck Cld-Mngd 24-port mGbE UPoE switch Meraki MS390-48UX2 L3 Stck Cld-Mngd 48-port 5GbE UPoE switch Fortinet FortiGate Ruckus Wireless, Inc. ICX7150-24-POE, SPR08090b 50-Port Gigabit PoE Smart Switch Viptela SNMP agent
724820	Ruckus Wireless, Inc. ICX7850-48FS Dell EMC Networking OS10 Enterprise, System Type: S5212F-ON Ruckus Wireless, Inc. ICX7650-48F HVC-Budel-FW01 Brocade Communications Systems, Inc. ICX7250-24, labeled as SPS08030

Ticket #	Vendor (9.1.2.0128)
	Brocade Communications Systems, Inc. FWS648G-POE, labeled as FWSL07400d1
	Ruckus Wireless, Inc. ICX7150-C08-POE, labeled as SPS08091
	Dell Networking OS, Series: MXL-10/40GbE
	Cisco IOS Software, C2960CX

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 Dell EMC Networking N1108P-ON Ruckus Wireless Inc (C) 2006 SG350-52 52-Port Gigabit Managed Switch Cisco Sx220 Series Switch Dell EMC Networking N3024ET-ON Cisco IOS Software, C880 Meraki MS355-24X Cloud Managed Switch Cisco Adaptive Security Appliance Version 9.12(3)12 SG250-08HP 8-Port Gigabit PoE Smart Switch
695460	Cisco NX-OS(tm) n9000 ProCurve 516733-B21 6120XG Blade Switch CBS350-8FP-E-2G 8-Port Gigabit PoE Managed Switch SF250-24 24-Port 10/100 Smart Switch SG250-26P 26-Port Gigabit PoE Smart Switch Ruckus Stacking System ICX7650-48Z-HPOE 24-port 10/100 Ethernet Switch Arista Networks DCS-7260CX3-64 Arista Networks DCS-7280SR-48C6 SG200-26FP 26-Port Gigabit PoE Smart Switch SG200-18 18-Port Gigabit Smart Switch Arista Networks CCS-758-CH Ruckus ICX7150-C08PT Cisco IOS Software, C1700 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) Note: SFTP has been deprecated and connections will fail using this option. SFTP will be removed from the drop down menu in a later release.

End of Support/End of Life

Fortinet is committed to providing periodic maintenance releases for the current generally available version of FortiNAC. From time to time, Fortinet may find it necessary to discontinue products and services for a number of reasons, including product line enhancements and upgrades. When a product approaches its end of support (EOS) or end of life (EOL), we are committed to communicating that information to our customers as soon as possible.

End of Support

Agent

Versions 2.x and below of the Fortinet Agent will no longer be supported. FortiNAC may allow the agent to communicate but functionality will be disabled in future versions. Please upgrade to either the Safe Harbor or latest release of the Fortinet Agent at your earliest convenience.

Fortinet Mobile Agent for iOS will no longer be supported. It will be completely removed in a future version. EasyConnect features are not affected as they do not require an agent on iOS.

Software

When a code series has been announced End of Support, no further maintenance releases are planned. Customer specific fixes will still be done.

Hardware

Physical appliance hardware reaches end-of-support when the maintenance contract is non-renewed, or at the end of year 4 (48 months beyond purchase date), whichever is first.

Appliance Operating System

Fortinet relies on the CentOS organization to publish periodic bug fixes and security updates for the CentOS Distribution.

CentOS 5

Effective March 31, 2017, CentOS will no longer provide updates for CentOS 5. Any vulnerabilities found with CentOS 5 after March 31st will not be addressed. FortiNAC software releases will continue to be supported on CentOS 5 through December 31, 2018.

As of 2016 Fortinet's appliances are based on the CentOS 7 Linux distribution. New appliance migration options are available for customers with CentOS 5 appliances who require operating system vulnerability patches, maintenance updates and new features available on CentOS 7.

CentOS 7

Effective June 30 2024, CentOS will no longer provide updates for CentOS 7. Any vulnerabilities found with CentOS 7 after June 30th will not be addressed.

FortiNAC and Analytics software releases will continue to be supported on CentOS 7 through December 31 2026 or end of product life (whichever comes first). See Product Life Cycle chart for details.

(<https://support.fortinet.com/Information/ProductLifeCycle.aspx>)

End of Life

Software

When a code series has been announced End of Life, no further maintenance releases are planned. In addition, customer specific fixes will not be done. If experiencing problems with a version of FortiNAC in the code series, you would be required to update before any issues can be addressed.

With the release of FortiNAC Version 8.5.0, Fortinet announced the End-Of-Life for FortiNAC 8.1. Existing customers under maintenance are strongly encouraged to upgrade to the current Safe Harbor release.

Considerations are as follows:

- FortiNAC Versions 7.0 and higher are not supported on appliances running firm-ware Version 2.X (SUSE) because of the limitations of this operating system and the hard-ware on which it is installed. Please contact your sales representative for hardware upgrade options.
- If you attempt to install FortiNAC Versions 7.0 and higher on an unsupported Operating System and hardware combination, the install process displays the following message: "This release is not supported on 1U SUSE-Linux appliances (firmware 2.x). The install process will exit now. Please contact Fortinet at: +1 866.990.3799 or +1 603.228.5300"
- On July 13, 2010 Microsoft ended support for Windows 2000 and Windows 2000 Server. These Operating Systems will be removed from the list of options in the Scan Policy Configuration screens in a future release.

Numbering Conventions

Fortinet is using the following version number format:

<First Number>.<Second Number>.<Third Number>.<Fourth Number>

Example: 8.0.6.15

- First Number = major version
 - Second Number = minor version
 - Third Number = maintenance version
 - Fourth Number = build version
-
- Release Notes pertain to a certain version of the product. Release Notes are revised as needed. The Rev letter increments accordingly. For example, updating the Release Notes from Rev C to Rev D indicates changes in the Release notes only -- no changes were made to the product.
 - The next number represents the version in which a Known Anomaly was added to the release notes (for example, V8.0).



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.