



FortiNAC - Release Notes

Version 9.2.0.0409

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

September 22, 2021

FortiNAC 9.2.0.0409 Release Notes

49-920-748698-20210922

TABLE OF CONTENTS

Overview	4
Important	4
Supplemental Documentation	4
Version Information	4
Compatibility	6
Agents	6
Web Browsers for the Administration UI	6
Operating Systems Supported Without an Agent	6
New Features	7
New Features in 9.2.0	7
Enhancements and Addressed Issues	8
Version 9.2.0	8
Device Support	18
Version 9.2.0	18
Numbering Conventions	21

Overview

Version 9.2.0.0409 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.
- 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](#).

- 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: 9.2.0.0409

Agent Version: 5.3.0.77

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

Many of the views in FortiNAC are highly dependent on JavaScript. The browser used directly impacts the performance of these views. It is recommended that you choose a browser with enhanced JavaScript processing.

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 9.2.0	7
------------------------------------	----------

New Features in 9.2.0

- Enhanced Appliance Installation: Login to the Administration UI in order to apply license key, configure appliance network settings and the FortiNAC Service Interface (eth1). There is no longer a separate UI.
- Ability to add Custom Endpoint Fingerprints using the REST API.
- New Endpoint Fingerprints view (Replaces Device Identity view) and Tasks view.
- Local RADIUS Server Enhancements
 - Updated views including configuration subsections
 - Multiple virtual Local RADIUS Servers
 - Multiple Winbind instances
 - Improved debugging tools
 - Improved visibility of services and configuration
 - Added support for EAP-FAST in FreeRADIUS to the extent possible:
Configurable EAP-FAST controls:
 - PAC Opaque Key
 - Allow Anonymous In-Band PAC Provisioning
 - Allow Authenticated In-Band PAC Provisioning
- Dashboard Rework
 - Multiplicity - Multiple Dashboards may now be created and the name may be freely modified. Dashboards may have multiple instances of each Widget.
 - Layout and Sizing - Widgets (formerly known as panels) are rendered in a row with a number of columns available based on the screen size. The row wraps automatically, filling from the left. All Widgets have a fixed height, but user adjustable width set to the number of columns they should span.
 - New Tiles for Pending Tasks and Endpoint Fingerprints.
- Persistent Agent Enhancements (Agent 5.3)
 - Agent included in FortiNAC 9.2
 - Agent fingerprints are now visible in the Endpoint fingerprints view
 - See 5.3 Agent Release notes for details and other enhancements
- FSSO Enhancements
 - User definable network address objects and address groups for SSO messaging.
 - Support for managing hosts with PA installed but not seen as connected by FortiNAC by a managed device.
 - Support for new dynamic firewall address API that will replace the FSSO protocol in FGTs running FOS 7.0.2
- Netflow protocol support added for Device Profiling..

Enhancements and Addressed Issues

These changes have been made in FortiNAC Version 9.2.0. These enhancements are in addition to the enhancements that are outlined in previous releases.

Version 9.2.0

Ticket #	Description (9.2.0.0409)
518423	802.1x support for Aerohive SR2208P
522462	Trigger "System Created Uplink" Events for Learned and User created Uplinks
543215	Make change in mib to not use Native Vlan on Juniper EX switches
594554	VLAN Switch Success Event and Alarm to contain the "from" and "to" VLAN information
600122	Add a configurable delay after receiving a warm start/cold start trap before FortiNAC engages with a switch
601831	Added support for Swagger Editor (used by FortiOS)
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.
640641	The dashboard is not showing any Mac agents. The total agents reflect the correct number but the mac column is zero.
650216	Unable to set firewall tags for PaloAlto model
650626	FortiNAC System Date Format changed to YYYYMMDD_HHMMSS.
659675	Provide Location (switch/AP and port), IP address, and "Connected Container" information into the "Rogue Connected" and "Device Created" events.
663957	Alcatel 6560 not switching VLANs
665011	Added support to configure multiple Local RADIUS Servers
666660	If a shared filter has an ! in it, a delete or edit silently fails
671704	FortiGate VPN Host is incorrectly registered as a device with no "Registered To" information and with "NAC-Default" Role
671997	Juniper Flex-CLI not working due to 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.
675847	VPN Model Configuration screen authentication method now displays LDAP checked by default.
676232	Host with a disabled logged on user is not moved to dead end.

Ticket #	Description (9.2.0.0409)
677981	Improved multiple VDOM support for FortiGate VPN integrations. Previously, FortiNAC was unable to determine correct tags to apply to sessions
682525	Unable to register MS Intune endpoints that only have an ethernet adapter
684657	Improved the communication method between Control Manager (NCM) and pods by using REST API and certificate client authentication over HTTP Requirements: - Manager must be installed with License key containing certificates (not required for pods). For more information see related KB article FD52784 - Firewalls allow TCP port 8443 between Manager and pods If the above requirements are not met, the Manager will use original communication methods
685763	Changed Proxy Radius logic for VDOM lookup to use VDOM from attribute Fortinet-Vdom-Name if present in auth request
688265	Account Requests > Approve Request doesn't close the overlay on success
689104	Send separate Emails for guest registration details and password
691837	Add GUI functionality to enable or disable masquerading e-mail as other addresses
691918	Improved Local RADIUS/winbind service operation visibility and debugging in GUI
692461	Modifying group members not shown in admin auditing logs
692995	Improved Dashboard view
693625	Groups service does not check for usage across different configurations
696239	Port Channel Support for HP Switches
696640	Access to gui is randomly lost
697296	Add vendorCodes directory to System Backup
698090	Fortigate L3 polls do not support reading IPv6 arp data
698728	Telnet/SSH to a FortiGate fail when post-login-banner is enabled
699606	A warning message now appears when attempting to install a legacy (NetworkSentry) license key using the UI
700276	Add Contact Status Polling for Link Mode FortiSwitches.
700580	Fortigate L3 Poller throws exceptions for static arp entries
700580	When polling the Fortigate, if there are multiple ARP entries for the same MAC address, the newest entry may not be used.
700610	Kiosk Page is Not Loading
701378	All API requests to a FortiGate fail when the post-login-banner is enabled
701764	Portal - Self Reg Pending view not visible when instructions are set to be inline
702259	Hostname information collected from FortiGate firewall sessions is no longer used for updating rogue host records. The information was sometimes inaccurate

Ticket #	Description (9.2.0.0409)
702941	Query OUI, FortiGuard and NMAP for every new rogue
705017	Settings > System Communication > Incorrect help text for Message Templates
705845	Searching groups by name in Roles and Network Device Roles views doesn't work
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
707284	VLAN ID and VLAN Name drop-down menu contents are now sorted in the Model Configuration View
708635	WinRM/WMI PowerShell Command Restriction by McAfee EDR - EncodedCommand
708649	Added Local RADIUS Server support for EAP-FAST. For details, see Administration Guide
708651	Added support to authenticate Cisco Access Points using EAP-FAST and dynamically provision network access.
708652	New Device Profiling Method: ability to check certificate field to classify hosts & devices
709269	FortiGuard Device Profiling method is not available on the Control Manager (NCM)
709278	Secondary Server in High Availability responds to RADIUS after Primary Server resumes control
709293	Added support to display FortiAnalyzer connection state
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
709447	The text on the social login buttons sometimes spills over edge
709464	Appliance installation is now done through the Administration UI as opposed to a separate Configuration Wizard
709559	Mist AP L2 Polling failure
709561	Passive Agent Policy group pull down does not show any AD groups if one of the AD servers is not reachable
709661	Automated identification of potential L3 sources post device discovery
709861	Added support for new API introduced in FortiGate/FOS version 7.x
709965	Server List panel in Control Manager Dashboard takes several minutes to build
710408	Implement new FortiGate v7 FSSO REST API
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.

Ticket #	Description (9.2.0.0409)
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
711377	Support for tunneling REST API requests over CSF
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	Misleading password configuration pop-up box in High Availability configuration
712658	Network Inventory takes a long time to load
712678	Clicking on a user count in the user summary panel on the dash board does not create a Filter when it opens Host View.
712695	Administration UI authentication fails when using a "+" sign in the password
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
713181	Added an import button to enable uploading hosts from an external file into the datatable.
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.
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 support for Versa router
714399	Exception during modeling leads to Cisco in locked state
714641	Device Identity view has been replaced with Endpoint Fingerprints view. Located under Users & Hosts > Endpoint Fingerprints . See new features.
714692	Removed iOS and Android from the "Add Device Profiling Rule" view.
714694	New Fingerprint database to accommodate multiple fingerprint sources. Data is displayed via the new Endpoint Fingerprints view.
714702	Not reading L3 from all VDOMs on a FortiGate.
714764	New install>Need a way to upload a license key from the client file system
714768	Fixed mapping for Alcatel-Lucent Enterprise OS6860E-P24

Ticket #	Description (9.2.0.0409)
714808	Ruckus L2 poll does not work with version 6
714947	FOS group dynamic firewall address (FSSO) integration
714954	Adding Virtual and Virtual Guest options to adapter Media Types
715251	When RadiusManager debug is enabled and an unknown RADIUS attribute is received, NullPointerException is printed and FortiNAC stops processing the request
715302	Added the "screen" command to the repository and image
715316	FSSO Race condition leaves some hosts with incorrect logon status
715418	Fix debug in TrapHandler to not mislead on linkup vs linkdown traps
715678	Introduce USG SKUs to restrict contact FortiGuard server, FDN Server and FortiNAC software download server in US only
716371	IllegalArgumentException thrown in PersistentAgent#isLinkLocal when called with an IPv6 address
716411	FSSO tags are not sent when host role changes.
716599	FortiNAC drops RADIUS packets at times of peak usage
716603	Fix scripts to make them POSIX compliant
716897	System>Settings>Trap Mib Files throws exception and does not function
717912	Group Membership performance is too slow to handle load from policy engine
718168	Add a convenience method to modify a local users password
718402	SvgIconInterface isnt being loaded properly during build
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 run install.bin if have legacy license key without High Availability
719780	Catch All rule name in Device 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"
720204	Updated FortiNAC log schema for FortiAnalyzer
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 should support the mac_list property in the API

Ticket #	Description (9.2.0.0409)
720471	Added cyber-blue MAC address 00:1A:7D:DA:71:15 to IgnoredAdapters.txt (Custom Ignored Adapters List)
721204	Added Mac Notification support for Dlink Switches
721566	Custom Scans Registry-Keys view produces an error
722811	In MDM integrations, fingerprints are now created with the hostName, OS or entity values for the host instead of updating the host record directly. These are viewable in the new Endpoint Fingerprint view
723107	Add Fingerprint from Persistent Agent data. These are viewable in the new Endpoint Fingerprint view
723563	Event Alarm Mapping not adding %host% or %event% information to Email Action
723851	DHCP Fingerprint for Mac OSX Bug Sur missing
724173	Fix CoA on Fortigates with FortiLink switch, where secret is defined on the switch
724363	Duplicate online hosts with same mac address are displayed under Adapters in Topology view.
724383	FNAC sometimes failed to poll some clients connected to FGT/FSW FOS7.0.
724769	Edit Role -> Groups -> Groups arent filtered
725009	Imported LDAP group does not map to Administrators
725360	Fix potential ClassCastException in MibObject
725604	Host is auto approved by FortiNAC even when an approver is configured in Standard User Login Portal.
725629	Unable to properly manage Aruba 9012 WLC due to incorrect mapping
725746	Communication issues between Control Manager (NCM) and POD causing Endpoint Compliance 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 doesnt accept new time format
725972	Remove unnecessary startup RelationInterface message from output.master
725981	LEAP support has been removed from the Local RADIUS Server configuration
726024	GA Renumber failed due to attempting to create + push existing tag
726099	FSSO processing performance enhancements
726329	Appliance installation is now done in the Administration UI. There is no longer a separate UI
726329	Basic Network config wizard page control alignment is off, no need for multiple columns.
726410	When a FortiLink Switch is renamed, the device and port model names in FortiNAC are not updated.

Ticket #	Description (9.2.0.0409)
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
726694	A Fingerprint is now created when FortiNAC updates a host record after reading the FortiGate Firewall Session table.
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
727831	Fingerprint attributes are not returned via REST get requests
728160	MySQL Exception Incorrect integer value: 'GuestSelfRegistration' for column 'sendPasswordSeparately' in output.master
728406	Proxy RADIUS packet debug - attempts to convert non-human readable octet string attrs, clutters output
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
728862	Enhanced DeviceImport CLI tool including SNMPv3 support. For details on all options, type "DeviceImport" in the CLI
729007	NullPointerException during V3 device creation via API when no v1 community strings provided
729421	Enhanced device type classifications based upon OUI
729585	Cisco ASA VPN clients not moved to the unrestricted group due to multiple values returned when reading object-group
729599	Obtrusive error popup thrown upon navigation to Topology view
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

Ticket #	Description (9.2.0.0409)
730857	No error message when DHCP scopes fail to import from file
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 configured
731580	Exception is displayed in server log during initialization
731597	Exception is logged when no devices present
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
732614	Clicking Read VLANs on Model Configuration view fails due to not-a-function error
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
735553	CLI and Vlan switching not functioning for Allied and Rugged devices
735791	Secondary servers do not retain contract entitlements
736110	Excessive exceptions for DatabaseObjectAlreadyExistsException seen in logs
736125	Added Netflow protocol support for Device Profiling
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

Ticket #	Description (9.2.0.0409)
736796	Added L3 Device Identification UI.
737244	Add REST API call to confirm device profiling rule in DeviceIdentityService
737732	FortiGate FSSO functionality is now configurable using address scopes and address groups for more flexible configuration
737740	Added PolicyHelper debug control / visibility to RADIUS log UI for improved troubleshooting
737779	Added ability to configure CLI Passwords using the Administration UI
738093	ISO build missing bc package
738096	Add checkboxes to support proactive nmap and Fortiguard method profiling
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
738388	Debug was added to indicate when System > Settings > Updates > System protocol is set to SFTP. This protocol has been deprecated
738721	Device Identity view has been removed
738805	Unable to set SSH port on Device Credentials page in version 9.1.2
739112	Improved default level log output to include more informative messages
739131	Need to replace mysql-connector
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
740723	Devices with VDOMs that specify local radius server/secret and use the mgmt IP - on restart the nas DB tbl entry is removed
740749	Local RADIUS can only handle secrets of 60 characters or less
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
741952	No response in UI when adding new network devices
741954	Add ability to read ethernet adapter for Google GSuite devices
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()

Ticket #	Description (9.2.0.0409)
742261	NullPointerException in ProbeTelnet.getProbeObjectsByInetAddress()
742347	IndexOutOfBoundsException in BridgeManager.VlanVerifyVector.put()
742861	More granular OS information collected from agents. Displayed in Agent Fingerprints
743381	Missing description for Radius in System/settings/Authentication/Radius
743535	License for jersey packages is listed incorrectly as EPLv2/GPLv2 in Help > Legal view
743543	Caching of dot1qIDtoVIDMappings not working on Juniper switches
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
744371	Fixes potential performance issue in table views.
745083	Control Manager (NCM) Sync fails with ArrayIndexOutOfBoundsException
745133	SSH is intermittently failing to some Cisco devices
709030	Improved the speed of Device Discovery
710957	
716411	FortiGate VPN hosts marked At Risk do not trigger a network change. FSSO device
715316	synchronization doesn't work properly with VDOMs.
717912	Group Membership performance is too slow to handle load from policy engine
715316	
733892	LicenseTool APPLIANCE shows EFFECTIVE count/level/certs if both are requested
733914	
733903	Setting Host Expiration field to "Never" resulted in inaccurate expiration dates (example 12/31/1969)
735520	Agent 5.3.0 package included
729033	
731645	
731193	
728989	
739380	AirWatch does not retrieve all MAC addresses for enrolled devices
745058	
742929	<p>The number of Operating System and Anti-Virus program options in the Scan Configuration have been reduced. Only those currently supported or commonly in use are now listed. Systems initially installed with 9.2.0 will have this change applied by default. Upgrades will have this functionality enabled upon the first auto-definition sync.</p> <p>For a list of available Operating Systems and Anti-Virus programs, see KB article FD53449. https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD53449</p>

Device Support

These changes have been made in FortiNAC Version 9.2.0. These are in addition to the device support added in previous releases.

Version 9.2.0

Ticket #	Vendor (9.2.0.0409)
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
706225	Ruijie XS-S1960
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
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

Ticket #	Vendor (9.2.0.0409)
	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 Networking OS Series: PE-FN-410S-IOM 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
721009	Added missing property for Viptela devices
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 Brocade Communications Systems, Inc. FWS648G-POE, labeled as FWSL07400d 1 Ruckus Wireless, Inc. ICX7150-C08-POE, labeled as SPS08091 Dell Networking OS, Series: MXL-10/40GbE Cisco IOS Software, C2960CX
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

Ticket #	Vendor (9.2.0.0409)
	Aruba JL676A 6100 48G 4SFP+ Aruba JL679A 6100 12G CL4 2SFP+ Dell S5048F-ON Brocade ICX7150-48-POE Brocade ICX7150-48-POEF HPE OfficeConnect 1950-24G-2SFP+-2XGT Huawei S5735-S48P4X Cisco NX-OS(tm) n5000
734133	Pnetworks switch
735445	Huawei Quidway S3352P-EI Huawei Quidway S9306
743833	Cisco Nexus(Cisco NX-OS(tm) nxos.9.3.5.bin) Cisco Nexus (Cisco NX-OS(tm) nxos.7.0.3.I7.9.bin)
745113	Dell EMC Networking OS S5730-68C-PWR-SI-AC Huawei Versatile Routing Platform Software VRP 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
689049	Dell Switch S4128T (DellSwitchOS10)

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© 2024 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.