FortiNAC - Release Notes

Version F 7.2.4

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

October 24, 2023
FortiNAC F 7.2.4 Release Notes
49-922-769106-20211216

TABLE OF CONTENTS

Change log

Date	Change description
August 3, 2023	Initial release.

Overview of Version F 7.2.4

- Build number: 0094

Notes

- Starting from 9.1.0, FortiNAC uses a new GUI format. FortiNAC cannot go backwards to a previous version. Snapshots should always be taken on virtual appliances prior to upgrade.

  

  Post 9.4, FortiNAC re-versioned. The first release after re-versioning is F 7.2. Hence, the order of releases is:
  FortiNAC 9.1 > FortiNAC 9.2 > FortiNAC 9.4 > FortiNAC F 7.2

- Critical information about upgrading your FortiNAC should be viewed in Upgrade Requirements.
- For upgraded FortiNAC devices running CentOS, use the sysinfo command; for newly deployed FortiNAC F 7.2+, issue `get system status` within the admin CLI.
- To review software version information via CLI:
  Appliances running on CentOS: type `sysinfo`
  Appliances running on FortiNAC-OS: type `get system status`
- For upgrade procedure, see the applicable cookbook in the Fortinet Document Library:
  OS and Software Upgrade (CentOS)
  OS and Software Upgrade (FortiNAC-OS)

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: F 7.2.4

Agent Version:

- MacOS: 10.7.1.9
- Windows & Linux: 9.4.3.100

Agents ship independent of product. For the latest Agent release notes, please see
- MacOS: 10.7.1.9
- Windows & Linux: 9.4.3.100

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: 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.

Upgrade Requirements

Ticket #	Description
FortiNAC License Key	Upgrading to this release requires the FortiNAC License. It is possible, however unlikely, older appliances may not have this specific type of license key installed. In such cases, an error will display during the upgrade. For additional details, see KB article https://community.fortinet.com/t5/FortiNAC/Troubleshooting-Tip-Upgrade-fails-with-license-requirement-error/ta-p/246324
Upgrade Path Requirements	Systems on version 9.1.6 must upgrade to either: • Higher version of 9.1 (e.g. 9.1.7) • 9.2.4 or higher Systems on versions 8.2 or lower must upgrade to 8.3 before upgrading to 8.4 or higher.
Legacy SSH Ciphers	Vulnerable Diffie-Hellman SSH Ciphers were removed from versions 9.2.8, 9.4.4. F7.2.3 and greater. The removal of these ciphers can cause SSH communication to fail between FortiNAC and network infrastructure devices still using these legacy ciphers. Depending upon the device, resulting behavior can vary from failing L2 and L3 polling to failing VLAN switching. The following events would be generated for the affected device: • L2 Poll Failed • L3 Poll Failed • VLAN Switch Failure The legacy ciphers must be re-added to FortiNAC via the CLI after upgrade. For details, see KB article https://community.fortinet.com/t5/FortiNAC-F/Troubleshooting-Tip-SSH-communication-fails-after-upgrade-due-to/ta-p/281029
892856	High Availibility and FortiNAC Manager Environments: The following are required as of 7.2.2: Key files containing certificates are installed in all FortiNAC servers. License keys with certificates were introduced on January 1st 2020. Appliances registered after January 1st should have certificates. To confirm, login to the UI of each appliance and review the System Summary Dashboard widget (Certificates = Yes). If there are no certificates, see Importing License Key Certificates in the applicable FortiNAC Manager Guide. Allowed serial numbers: Due to enhancements in communication between FortiNAC servers, a list of allowed FortiNAC appliance serial numbers must be set. This can be configured prior to upgrade to avoid communication interruption. For instructions, see What's New.
834826	As of FortiNAC versions 9.4.2 & vF7.x, Persistent Agent communication using UDP 4567 is no longer supported.

Ticket #	Description
	It is recommended the following be checked prior to upgrade to avoid agent communication disruptions: • SSL certificates are installed for the Persistent Agent target • Persistent Agents are running a minimum version of 5.3 For additional details see KB article 251359. https://community.fortinet.com/t5/FortiNAC/Technical-Note-Agent-communication-using-UDP-4567-no-longer/ta-p/251359
885056	All devices managed by FortiNAC must have a unique IP address. This includes FortiSwitches in Link Mode: Managed FortiSwitch interface IP addresses must be unique. Otherwise, they will not be properly managed by FortiNAC and inconsistencies may occur. This is also noted in the FortiSwitch Integration reference manual.

Pre-upgrade Procedures

Enhancements were made to the communication method between FortiNAC servers for security. Due to this change, all servers must have additional configuration in order to communicate. The following procedure should be done prior to upgrade to prevent communication interruption.

Follow the instructions for the appropriate appliance:

- Pre-upgrade procedure (FNC-M-xx/FNC-CA-xx): FortiNAC appliances running on CentOS
- Pre-upgrade procedure (FNC-MX-xx/FNC-CAX-xx): FortiNAC appliance running on FortiNAC-OS

Pre-upgrade Proceedure (FNC-M-xx/FNC-CA-xx)

This configuration applies to FortiNAC version 7.2.2 and greater.

Configure all servers to allow communication between each other. This is done using an attribute that lists all the allowed serial numbers with which appliances can communicate.

Steps

1. Confirm key files containing certificates are installed in all FortiNAC servers.
   Administration UI Method:
   The **System Summary Dashboard** widget should show 'Certificates = Yes'.
   CLI Method:
   Virtual appliance: Log in to the CLI as root and type:

   ```
   licensetool
   ```

   Physical appliance: Log in to the CLI as root and type:

   ```
   licensetool -key FILE -file /bsc/campusMgr/.licenseKeyHW
   ```

   Response from the above commands should show:

   ```
   "certificates =[xxxxxxxxxxxxxxxxxx,xxxxxxxxxxxxxxxxxx]".
   ```

   If '`certificates = []`' or there is not a 'certificates' entry listed at all, keys with certificates must be installed. See Importing License Key Certificates in the FortiNAC Manager Guide.
2. Compile the allowed serial number list. In a text file (Notepad, etc), document the serial numbers of each appliance. Serial numbers can be obtained in the following ways:
   - Customer Portal (https://support.fortinet.com)
   - System Summery Dashboard widget in the Administration UI of each appliance
   - CLI of each appliance using licensetool command

   Example:
   FortiNAC Manager A (primary) & B (secondary)
   FortiNAC-CA servers A (primary) & B (secondary)
   FortiNAC-CA server C

Record serial numbers for:
FortiNAC Manager A: FNVM-Mxxxxx1
FortiNAC Manager B: FNVM-Mxxxxx2
FortiNAC-CA server A: FNVM-CAxxxxx4
FortiNAC-CA server B: FNVM-CAxxxxx5
FortiNAC-CA server C: FNVM-CAxxxxx6

3. In the same text file, write the following command, listing all the serial numbers recorded in step 2:
   Command:

   ```
   globaloptiontool -name security.allowedserialnumbers -setRaw
   "<serialnumber1>,<serialnumber2>,<serialnumber3>"
   ```

   Example

   ```
   globaloptiontool -name security.allowedserialnumbers -setRaw "FNVM-Mxxxxxxx1,FNVM-
   Mxxxxxxx2,FNVM-CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6"
   ```

4. Perform the following steps on all servers:
   a. Log in to the CLI as root.
   b. Paste the `globaloptiontool` command from the text file.
   Note:
   - The message "Warning: There is no known option with name: security.allowedserialnumbers" may appear. This is normal.
   - In High Availability configurations, only the Primary Server need to have the command entered. Database replication will copy the configuration to the Secondary Server. Using the above example, CLI configuration would be applied to Manager A.

     Example

     ```
     > globaloptiontool -name security.allowedserialnumbers -setRaw "FNVM-
     Mxxxxxxx1,FNVM-Mxxxxxxx2,FNVM-CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6"

     Warning: There is no known option with name: security.allowedserialnumbers

     New option added
     ```

   c. Confirm entry by typing:

   ```
   globaloptiontool -name security.allowedserialnumbers
   ```

   Example

   ```
   > globaloptiontool -name security.allowedserialnumbers

   Warning: There is no known option with name: security.allowedserialnumbers

   122 security.allowedserialnumbers: FNVM-Mxxxxxxx1,FNVM-Mxxxxxxx2,FNVM-
   CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6
   ```

5. Log out of the CLI. Type:
   `logout`

You have completed the pre-upgrade procedure.

Pre-upgrade procedure (FNC-MX-xx/FNC-CAX-xx)

This configuration applies to FortiNAC version 7.2.2 and greater.

Configure all servers to allow communication between each other. This is done using an attribute that lists all the allowed serial numbers with which appliances can communicate.

Steps

1. Compile the allowed serial number list. In a text file (Notepad, etc), document the serial numbers of each appliance. Serial numbers can be obtained in the following ways:
   - Customer Portal (https://support.fortinet.com)
   - System Summery Dashboard widget in the Administration UI of each appliance
   - CLI of each appliance using get system status command

   Example:

   FortiNAC Manager A (primary) & B (secondary)

   FortiNAC-CA servers A (primary) & B (secondary)

   FortiNAC-CA server C

   Record serial numbers for:

   FortiNAC Manager A: FNVM-Mxxxxx1

   FortiNAC Manager B: FNVM-Mxxxxx2

   FortiNAC-CA server A: FNVM-CAxxxxx4

   FortiNAC-CA server B: FNVM-CAxxxxx5

   FortiNAC-CA server C: FNVM-CAxxxxx6
2. In the same text file, write the following command, listing all the serial numbers recorded in the previous step:

   Command:

   ```
   globaloptiontool -name security.allowedserialnumbers -setRaw
   "<serialnumber1>,<serialnumber2>,<serialnumber3>"
   ```

   Example

   ```
   globaloptiontool -name security.allowedserialnumbers -setRaw "FNVM-Mxxxxxxx1,FNVM-
   Mxxxxxxx2,FNVM-CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6"
   ```
3. Perform the following steps on all servers:

   a. Log in to the CLI as admin and type:

   ```
   execute enter-shell
   ```

   Hit <ENTER>

   b. Paste the `globaloptiontool` command from the previous step.

   Note:
   - The message "Warning: There is no known option with name: security.allowedserialnumbers" may appear. This is normal.
   - In High Availability configurations, only the Primary Server need to have the command entered. Database replication will copy the configuration to the Secondary Server. Using the above example, CLI configuration would be applied to Manager A.

Example

```
> globaloptiontool -name security.allowedserialnumbers -setRaw "FNVM-
Mxxxxxxx1,FNVM-Mxxxxxxx2,FNVM-CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6"

Warning: There is no known option with name: security.allowedserialnumbers

New option added
```

c. Confirm entry by typing:

```
globaloptiontool -name security.allowedserialnumbers
```

Example

```
> globaloptiontool -name security.allowedserialnumbers

Warning: There is no known option with name: security.allowedserialnumbers

122 security.allowedserialnumbers: FNVM-Mxxxxxxx1,FNVM-Mxxxxxxx2,FNVM-
CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6
```

4. Restart FortiNAC services. Type:

```
shutdownNAC
```

<wait 30 seconds>

```
startupNAC
```

5. Log out of the CLI. Type:

```
exit

exit
```

You have completed the pre-upgrade procedure.

Compatibility

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

Example: 7.2.0.0035 cannot be downgraded to any other release.

Agents

FortiNAC Agent Package releases 5.x are compatible with FortiNAC Product release F 7.2.4. Compatibility of Agent Package versions 4.x and below with FortiNAC F 7.2.4 is 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	Symbian	Web OS	Windows
Windows CE	Windows Phone	Windows RT	

What's new in F 7.2.4

Important notice

Enhancements were made to the communication method between FortiNAC servers for security. Due to this change, all FortiNAC servers must have additional configuration in order to communicate. The following procedure should be done prior to upgrade to prevent communication interruption.

Follow the instructions for the appropriate appliance (if FortiNAC Manager is not used, these steps can be skipped):

- Pre-upgrade procedure (FNC-M-xx): FortiNAC appliances running on CentOS
- Pre-upgrade procedure (FNC-MX-xx): FortiNAC appliance running on FortiNAC-OS

Enhancements and Addressed Issues F 7.2.4

Ticket #	Description
889895	High Availability cannot be removed from FortiNAC GUI.
920942	Unable to re-sync interfaces on Cisco ASA when username is configured with privilege level 15.
819396	Incorrect rank information reported in Audit Log.
932570	mibID parsing fails to check the type (sysObjectID) if the FirmwareVersion lacks a suffix.
754346	Port Changes filter parameters are not being retained.
904324	Default 'CN=Portal' Portal SSL Certificate is presented after reboot.
930027	The portal SSL setting doesn't remain enabled after a restart of NAC services or failover and return to primary control.
937147	Port2 remains active on the primary server after a failover to secondary.
944475	Routes aren't dynamically created for scopes in the configWizard.
948598	There's an L2 polling loop when reading L2 Data from FortiGate.
951943	Device profiling rules fail due to the 'TCPPortMethod IP not initialized' error when a host has a recent IP in ArpTool.
846822	FortiNAC's NMAP scan failed because of an old IP reported from the arptool.
865256	The Vendor OUI Device Type-based Device Profiling rule isn't functioning as expected.
884329	Base license, User/Host profiles, and Network Access Policies are producing permissions errors.
889986	There are issues when enabling and adding subnets in the "Require Connected Adapter".
891890	Windows 11 hosts are mistakenly detected as Windows 10 hosts when using the Dissolvable agent.
908857	The HA gateway is overwritten when making changes in the configWizard in Azure.
910706	Creating a guest account with REST v2 results in errors 400 and 500.
912115	The Guest Self Registration produces an error stating 'The input is required'.
918221	Host import fails to merge all sibling adapters.
920800	There are 404 errors when trying to request the physical MAC for a specific

Ticket #	Description
	host.
921705	A PA logged-on user is deauthenticated upon machine-based TLS authentication.
922114	Changes in nested group membership aren't logged in admin auditing.
923688	The Self Guest Registration Page with Dissolvable Agent doesn't redirect to the Success Page after scanning.
925641	There's a need to provide full support for the Adtran NetVanta 1234 switch.
926429	The MDM API URL displays 'Page Not Found'.
929383	The FNAC-F initial setup fails when an admin GUI password containing the '&' character is used.
930765	FortiNAC doesn't process MAC notification traps from Aruba CX 6000.
931408	The HTTP cookie is missing a Secure attribute on port 80.
934696	Group data becomes corrupted after FNAC starts up.
938146	Hosts registered in gSuite with common ethernet adapter host records are being overwritten.
938165	There's an option to skip FQDN parsing during device discovery.
939122	FortiNAC is unable to read an endpoint's vulnerability status from FortiEMS.
941207	Portal SSL switches to "Disabled" after every system restart.
942642	The Ruckus Integration doesn't support VLE with a large number of SSIDs.
942686	Unable to retrieve a grab-log-snapshot when the secondary system is running and in control.
942947	Uncompressed database backup replication to the secondary server results in 100% disk usage.
945416	FortiNAC is unable to apply CLI configurations to the Huawei Switch S5720-28X-PWR-SI-AC.
946405	The scheduler's popup dialog box displays a CLI Configurations error: a.name is undefined.
948193	Applied filters in Network>Port changes aren't saved after updating the selection.
953226	Machine Authentication using MSCHAPv2 can't be completed.
783304	The DHCP responds with unexpected addresses in the DHCP-Server-Identifier, causing release/renew failures.
889609	The switch port doesn't dynamically change to uplink when a v-edge router is directly connected to a Cisco switch port.

Ticket #	Description
904624	The host summary panel doesn't accurately display the total host count.
907355	Errors in the messaging for High Availability Configuration.
907504	Error message when trying to add a server to NCM.
908777	The GUI CLI Configuration for Logical Network in Model Configuration isn't applied correctly.
917032	MICROSENS G6 Switch has issues with hiding macs on the link feature.
917610	The updated dialog box is presented when the root CLI password is changed.
919423	The API endpoint '/host/scan' returns a status code of 405 (Method Not Allowed) for POST requests.
920334	VLAN changes aren't reflected correctly on FNAC inventory when integrated with FSW.
926831	When a laptop is connected to a dock with a Persistent Agent installed, the 'managed by MDM' flag isn't displayed in FortiNAC.
927754	Custom Registration fails with the error message: 'Anonymous Guest Access is not enabled'.
930459	There are issues with FortiNAC's integration with Tellabs switches.
934685	FortiLink over P2P L2 results in FortiNAC not setting Uplink Ports.
936140	Entitlements are removed after an upgrade on a Managed Server with the .licenseKeyNCM in the old key format.
936704	The hotstandby.log, dhcpd.log, and named.log are included in the grab-log-snapshot.
937206	Devices are created using SNMPV1 when SNMPV2 is used to add the device.
942731	There's a permissions error when issuing the 'hsForceFailover' command.
944917	The ‘Clear Known Hosts’ feature doesn't work.
945086	L2 polling isn't functional on private VLAN-enabled Cisco-XE switches.
949524	Huawei Access Points (AP) aren't listed in the FortiNAC inventory.
953685	The secondary system takes control prematurely after ETH0 activates.
954095	The Groups page throws an HTTP 500 error.
955704	The vendor name 'Blink by Amazon' contains an extra space at the end.
955965	Access enforcement settings aren't applied for manually created logical networks when set to 'Deny' only.
958433	FortiNAC sends the API request for Ruckus SZ300 using the wrong port number.

Ticket #	Description
959178	The exec tcpdump doesn't display packets in real-time.
949915	RADIUS authentication fails due to permission issues.
947918	There are missing configurations for additional routes after setting up HA.

Known Issues Version F 7.2.4

Ticket #	Description
946405	Scheduler pop up dialog box with CLI Configurations error of undefined.
954220	Unable to restore system backup files on FortiNAC-OS appliances.
934794	Performance issues with host record aging.
970763	FortiNAC SSH client no longer supports the weaker sha1 based kex algorithms.
968100	Aggregate ports do not display in the FortiNAC UI for Dell EMC switches.
970763	FortiNAC SSH client no longer supports the weaker sha1 based kex algorithms.
969091	Admin with System Administrator profile cannot delete another user in the UI with Base license.
951419	HTTPS Status 500 - Internal Server Error attempting to access model config from right click context menu.
955985	Extreme switch with 'description-string' in switchport config won't display connected adapters in GUI device model.
968630	In High Availability configurations, disk fills on Primary and Secondary servers after a period of time due to large backup files.
970257	Specified role not assigned to devices registered via the Portal, instead NAC-Default is assigned.
970076	Extreme 4826GTS-PWR+ (OID: enterprises.45.3.78.1) CLI credentials fail to validate.
964841	Users & Hosts > Hosts GUI does not allow selection of bulk hosts in view.
730221	Support for Meraki Wired Switch Stacks.
827499	Show system interface does not show the eth1/port2 IP address for Forti-OS FNAC.
877245	When adding an LDAP Admin user, it is found in the directory, but the user dialog defaults to local.
962475	After the Failover test (hsForceFailover), the GUI's "Power Management" displays incorrect behavior for Reboot and PowerOff.
827283	The Roaming Guest Logical Network is missing from the Model Configuration of FortiGate and possibly from other vendors.
912555	The Sponsor Approval Link requires login for non-admin users.
916289	Aruba APs are observed moving between WLCs, triggering L2 polls at an exceptionally high rate.

Ticket #	Description
914051	The client accesses the 'no failed scans' remediation page; however, the host health status indicates a scan failure, leaving no possible actions for the user.
956436	FortiNAC does not function properly as a RADIUS proxy when integrated with a NEC-QX switch.
960060	"Device Link Down" and "Device Link Up" event log entries for link state traps do not display the correct interface value.

Device Support Considerations

Ticket #	Description
548902	Management of wired ports on Aerohive AP-150W controlled by AerohiveNG is currently unsupported.
679230	Aruba 9012-US currently not supported.If required, contact sales or support to submit a New Feature Request (NFR).
7680531	Ubiquiti Gen2 Unifi switches (example: USW-16-POE) are currently not supported. If required, contact sales or support to submit a New Feature Request (NFR).
	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, integration with Ubiquiti AirOS AP is not supported.Ubiquiti AirOS AP does not have the necessary capabilities to allow for full integration with FortiNAC. The limitations are as follows: - No support for external MAC Authentication using RADIUS. - Limited CLI and SNMP capability. No ability to dynamically modify access parameters (ie. VLANs) for active sessions.
	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.
	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 Version F 7.2.4

Ticket #	Vendor
918683	New device integration with TPLink TL-SG2428 switches.
935218	Huawei YunShan OS Version 1.22.0.1 (S5700 V600R022C01SPC500) Huwaei CloudEngine S5735-L48P4XE-A-V2 Hangzhou H3C Comware Platform Software, Software Version 3.10, Release 2211P06 H3C S3100-52TP-SI Cisco IOS Software [Cupertino], S5800 Switch Software (S5800-UNIVERSALK9-M) OAW-AP1301 4.0.5 OAW-AP1231 4.0.5 Huawei AirEngine5760-51 Huawei Versatile Routing Platform Software VRP software, Version 5.170 (AirEngine5760-51 V200R022C00SPC100) Hirschmann MAR Juniper Networks, Inc. ex4400-48mp Ethernet Switch, kernel JUNOS 22.2R3.15 Hirschmann Railswitch FortiGate Aruba Instant On 1930 48G Class4 PoE 4SFP/SFP+ 370W Switch JL686A, InstantOn_1930_1.0.2.0
939984	ArubaOS (MODEL: 274), Version 6.5.4.25-6.5.4.25 Cisco IOS Software [Amsterdam], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.5 Juniper Networks, Inc. ex4400-48mp Ethernet Switch, kernel JUNOS 22.2R3.15 Ruckus Wireless, Inc. ICX8200-48P-POE, IronWare Version 10.0.00T253
944007	ArubaOS (MODEL: 615), Version 8.11.1.1-8.11.1.1 SSR Cisco IOS Software, C3700 Software (AP3G2-K9W7-M), Version 15.3 (3)JH Cisco IOS Software, C3600 Software (AP3G2-K9W7-M), Version 15.3 (3)JF15 Aruba R0X24C 6405 v2 Chassis FL.10.10.1070 24-Port Gigabit PoE Smart Switch CBS250-48PP-4G 48-Port Gigabit PoE Smart Switch Huawei AR161FG-L Huawei Versatile Routing Platform Software VRP (R) software,Version 5.160 (AR161FG-L V200R005C20SPC200)
953269	IE1000 Industrial Ethernet Switch, Version: 1.8.2#2020-08-13T23:48:09+00:00 Core Switch

Ticket #	Vendor
	Ruckus Wireless Inc (C) 2006 Aruba Instant On 1830 24G 2SFP Switch JL812A, InstantOn_1830_2.8.0.0 (17), Linux 4.4.120, U-Boot 2013.01 (V1.0.0.21) DGS-1210-48 4.10.023 DGS-1210-28/C1 4.10.004 Aruba Instant On 1830 48G 4SFP Switch JL814A, InstantOn_1830_2.5.0.0 (48), Linux 4.4.120, U-Boot 2013.01 (V1.0.0.17) Aruba Instant On 1960 24G 2XGT 2SFP+ Switch JL806A, InstantOn_1960_2.8.0.0 (17), Linux 4.4.120, U-Boot 2013.01 (V1.0.0.27) HPE Comware Platform Software, Software Version 7.1.070, Release 6710P03 HPE FF 5945 2-slot Switch Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 17.9.1, RELEASE SOFTWARE (fc8)
957106	Palo Alto Networks PA-5400f series firewall Aruba R9W95A 8100-24XT4XF4C switch LL.10.12.0006 Aruba Instant On 1930 48G Class4 PoE 4SFP/SFP+ 370W Switch JL686B, InstantOn_1930_2.8.1.0 (35), Linux 4.4.120, U-Boot 2013.01 (V1.0.1.41) JetStream 8-Port Gigabit Smart Switch JetStream 8-Port Gigabit Smart Switch Alcatel-Lucent Enterprise OS6350-P10 6.7.2.191.R04 GA, June 20, 2018. SG550XG-24T 24-Port 10GBase-T Stackable Managed Switch Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 17.9.4, RELEASE SOFTWARE (fc5) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2023 by Cisco Systems, Inc. HPE Comware Platform Software, Software Version 7.1.070, Release 6330 HPE 5140 24G PoE+ 4SFP+ EI Sw Copyright (c) 2010-2021 Hewlett Packard Enterprise Development LP Extreme 210-Series 48GE, 4 1GbE SFP ports, 1 Fixed AC PSU, L2 Switching, 1.2.6.9, Linux 3.6.5, U-Boot 2012.10-00003-g56c397c (Mar 28 2017 - 15:11:08) CBS350-48T-4G 48-Port Gigabit Managed Switch S6720-32X-LI-32S-AC Huawei Versatile Routing Platform Software VRP (R) software,Version 5.170 (S6720 V200R011C00SPC200) Copyright (C) 2007 Huawei Technologies Co., Ltd. 5420M-48W-4YE-FabricEngine (8.10.1.0)
949565	Ruckus Wireless, Inc. ICX8200-24P-POE, IronWare Version 10.0.00T253 Ruckus Wireless, Inc. ICX7550-24F, IronWare Version 08.0.95gT241 Aruba Instant On 1930 24G 4SFP/SFP+ Switch JL682A, InstantOn_1930_2.8.1.0 (35), Linux 4.4.120, U-Boot 2013.01 (V1.0.1.41) Aruba Instant On 1930 24G Class4 PoE 4SFP/SFP+ 195W Switch JL683A, InstantOn_1930_2.8.1.0 (35), Linux 4.4.120, U-Boot 2013.01 (V1.0.1.41)

Ticket #	Vendor
	Aruba Instant On 1960 24G 20p Class4 4p Class6 PoE 2XGT 2SFP+ 370W Switch JL807A, InstantOn_1960_2.8.0.0 (17), Linux 4.4.120, U-Boot 2013.01 (V1.0.0.27) Meraki CW9164I Cloud Managed AP Juniper Networks, Inc. ex4400-48t Ethernet Switch, kernel JUNOS 21.2R2-S2.3, Hirschmann MACH4002 DGS-3000-28XS Gigabit Ethernet Switch CBS250-24P-4G 24-Port Gigabit PoE Smart Switch AP310 , Version 7.7.1.1-005R MIB=01a MYS001PJT1FW01 Huawei AirEngine5761R-11E Huawei Versatile Routing Platform Software VRP (R) software, Version 5.170 (AirEngine5761R-11E V200R021C00SPC200)
927791	Support Request for Ruckus 8200 Switch Series Version 10.0.00T253
951420	Huawei switch with new port format fails L2 polling
918683	Change end of line value to a carriage return for TP-Link switches Integration with TPLink TL-SG2428P.

System Update Settings

1. In the FortiNAC Administrative UI, navigate to **System > Settings > Updates > System**.
2. Update the appropriate fields to configure connection settings for the download server.

Field	Definition
Host	Set to fnac-updates.fortinet.net
Auto-Definition Directory	Keep the current value.
Product Distribution Directory	Set to Version_F7_2
Agent Distribution Directory	Keep the current value.
User	Set to updates (in lowercase)
Password	Credentials required. Default is not available.
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.

3. When the download settings have been entered, click **Save Settings.**

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 4.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.

Numbering Conventions

Fortinet is using the following version number format:

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

Example: 7.2.0.0035

- 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.