FortiNAC - Release Notes

Version F 7.2.8

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

November 12, 2024
FortiNAC F 7.2.8 Release Notes
49-922-769106-20211216

TABLE OF CONTENTS

Change log

Date	Change description
November 12, 2024	Initial release.

Overview of Version F 7.2.8

- Build number: 0149

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)

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 7.2.7

Agent Version:

- MacOS: 10.7.2
- Windows & Linux: 9.4.4

Agents ship independent of product. For the latest Agent release notes, please see
- MacOS: 10.7.2
- Windows & Linux: 9.4.4

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
931408	Under **Portal > Portal SSL** the "Disabled" option is no longer available as of FortiNAC v9.4.5, vF7.2.4 and vF7.4.0. If using this option, install SSL certificates in the Portal target prior to upgrade. See Certificate management in the Administration Guide.
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
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. 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.
829805	FortiNAC supports REST API V2. For a list of supported v2 calls see https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/845cfa28-d2a7-11ee-8c42-fa163e15d75b/rest-api-f-7.2-pdf.pdf As of FortiNAC version 7.2, all v1 calls have been deprecated except for the following:

Ticket #	Description
	• FortinetFabricIntegrationService • ServerInformationService • ServiceDocumentService • ControlService

Upgrade Path

Important notice

Version 9.1.7 may directly upgrade to 7.x, without any intermediary steps.

However, Version 9.1.6 *must* follow this path:

9.1.6 > 9.2.6 > 7.x

Current Version	Target Version	Upgrade Path Requirement	Ticket #
7.2.0	7.2.8	None	N/A
7.2.1			
7.2.2			
7.2.3			
7.2.4			
7.2.5			
7.2.6			
7.2.7			

Upgrade Considerations

Ticket #	Description
871265, 949927	Due to vulnerabilities, FortiNAC-OS does not currently support SAML/Shibboleth. Support is scheduled to be added in a future release.

Hardware Support

This section lists the hardware models supported by FortiNAC F 7.2.8 F.

- FortiNAC-CA-500F: FN500F
- FortiNAC-CA-600F: FN600F
- FortiNAC-CA-700F: FN700F
- FortiNAC-M-550F: FN55MF
- FortiNAC-CA-500C: FN5HCA
- FortiNAC-CA-600C: FN6HCA
- FortiNAC-CA-700C: FN7HCA
- FortiNAC-M-550C: FN55M

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 procedure (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 9.4.4 Windows, 10.7.2 Linux and macOS, F 7.2 Android and agent F 7.6.0 are compatible with this FortiNAC Product release.

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

Apple iOS	Chrome OS	iOS for iPod	Kindle
iOS for iPad	iOS for iPhone	Windows	Linux
FreeBSD	NetBSD	Open BSD	

What's new in F 7.2.8

There are no new features in FortiNAC F 7.2.8.

Resolved Issues F 7.2.8

Ticket #	Description
0963527	"Flush" button for Device profile rules returns "Request unsuccessful with no errors reported."
1090447	Unable to set right click menu model config for the registration VLAN.
1093080	System check repeatedly fails on the primary server after configuring the shared IP.
1094064	After restarting service, error "chmod: cannot access '/bsc/.ssh/id_ed25519.pub': No such file or directory"
1064753	Delay in Sending Disconnect Request for Huawei AC6508 WLC.
993873, 995406	Users & Hosts - Quick Search gives unexpected results in Hosts and Adapters views.
1089487	Config Wizard Error: Apply script interrupted apply did not complete.
1085862	FortiNAC cannot send SMS for some numbers over SelfGuestRegistration .
1084923	telnetMibs files re-written after reboot.
1081023	RADIUS authentication failing due to "no suitable signature algorithm".
1080122	RADIUS changes included to support FOS version 7.2.11, 7.4.6 and 7.6.1 requiring Message-Authenticator in response. Previously, FortiGates running these FOS versions would fail CLI/GUI RADIUS server connectivity test with FortiNAC. Note RADIUS client connectivity is not affected.
1074244	Secondary taking the server Identifier of the primary in dhcpd.conf.
1073990	C and A Migration to FortiNAC-OS adds Application Server as Secondary in Dashboard.
1073462	After setting up High Availability, secondary server hardware appliance shows a license level of UNLICENSED.
1071760	Hosts not being set as 'Managed by MDM' for multiple MDM's.
1071422	Admin GUI service fails to start due to missing TLSServiceConfiguration.
1071356	Mismatched/incomplete data from an AirWatch MDM poll.
1070780	Additional fixes for asymmetric routing flow on FortiNAC-OS.
1070490	Unable to filter using multi-search options.
1070488	FortiNAC Admin GUI failing to start on both Primary and Secondary FortiNAC Servers.
1069799	Custom filter is not applied if using “created After” filter option.

Ticket #	Description
1069796	Unable to register host to user if more than 1,000+ user accounts exist.
1068711	Missing the ldapsearch CLI tool in FortiNAC-OS.
1067692	Ruijie S6110-24MG4VS-UP - FortiNAC can not learn current VLAN or change VLAN.
1066558	API Request for User/Dashboard/Host-Summary Responds with "Permission Error".
1065681	FortiNAC memory usage incrementally increasing due to memory leak.
1064105	High memory utilization due to memory leak.
1061918	Error generated when downloading log snapshot.
1061842	Unable to retrieve SNMP Hardware Status Monitoring Information for FortiNAC-OS.
1060574	Unable to delete offline Managed CA's in Servers Dashboard Widget on FortiNAC Manager.
1059488	Enforcing authentication is bypassed when using local RADIUS.
1058175	Allow adding SSH Remote Backup port.
1056228	HP Comware Switch H3C CLI credentional validation failing.
1056183	L2 Polling does not work properly for DELL Switch`s 802.1x enabled ports.
1055219	Self Registration SMS notifications do not include the Subject line.
1054615	FortiGate SSL VPN integration user session logoff after 3-5 minutes.
1052831	FortiNAC does not display ONT interfaces of Nokia Switch ISAM 7350.
1050487	FortiNAC unable to model Cisco IE1000 Industrial Ethernet Switch.
1048902	Certificate Revocation Check does not work as expected.
1048537	Duplicate AP's created if DHCP is used to assign IPs to Mist AP's.
1045530	Model Configuration - Logical Network Information does not display for FortiGate 60F.
1045323	RADIUS authentication loop when unauthenticated and at-risk host connects to wired switch port.
1030100	Wired connection action state values set to "Bypass" via API display as "Enforce" in GUI.
1028912	FNAC is unable to interpret port ID from RADIUS in Dell EMC N2224X-ON switches.
1027524	CentOS to FortiNAC-OS migrations do not properly copy over the eth0 IP addresses for Primary and Secondary servers.

Ticket #	Description
1026068	Allied Telesis Switches AT-x530l, AT-GS950
1022348	Delays in dynamic address tag being sent due to host VPN adapter association.
1022276	Errors accessing Portal Configuration and Policy & Objects in the FortiNAC CA GUI.Occurs in the (uncommon) configuration where FortiNAC Manager and managed CA server both have subscription endpoint licenses applied but at different service levels (Plus vs Pro).
1018918	Prevent asymmetric routing with VPN integrations.
1013178	FortiNAC Manager unable to sync with High Availability pair where secondary server is in control.
1011825	High Availability failover due to RADIUS service health check timing out.
1010068	Inaccurate ports and VLAN assignments are displayed when securing a device using API.
1008427	Cannot update admin password for FortiGate Model via API .
1008097	Winrm "Windows Profile" Method if Failing due to java.io.EOFException: Unexpected end of ZLIB input stream.
992475	High Thread counts observed after upgrading to interim build.
989054	Host filter not working properly.
987401	Last Name and First Name are missing when exporting admin users.
963527	"Flush" button for Device Profile Rules returns "Request unsuccessful with no errors reported".
873131	Added the following API queries for FortiNAC Manager: /api/v2/host/ncm /api/v2/host/ncm/{hostID} /host/ncm/by-mac/{mac-address}

Common Vulnerabilities and Exposures

Visit https://www.fortiguard.com/psirt for more information.

Note: The following CVE's have been resolved, but security scanners may still flag some of them as vulnerabilities due to version-based detection methods.

Bug ID	CVE references
1057567	FortiNAC F 7.2.8 is no longer vulnerable to the following CVE reference. • CVE-2024-3596
1051904	FortiNAC F 7.2.8 is no longer vulnerable to the following CVE reference. • CVE-2024-6387

Known Issues Version F 7.2.8

Ticket #	Description
1099257	If SSH public-key authentication is enabled but not configured on the FortiGate, the FortiGate generates an error message after the initial failed login. For details and workaround, see article 360152. https://community.fortinet.com/t5/FortiNAC/Technical-Tip-How-to-disable-public-key-authentication-FortiNAC/ta-p/360152
1133813	Migrated legacy device types cause error when bulk importing hosts.
1099257	FortiGate generates an "invalid ssh key" message each time FortiNAC connects. FortiNAC first attempts login using the ssh-key public key. If login fails, the CLI password is used. This can cause the Fortigate to generate email alerts even though Validate Credentials is successful and SSH communication works. For a potential workaround, see article https://community.fortinet.com/t5/FortiNAC/Technical-Tip-How-to-disable-public-key-authentication-FortiNAC/ta-p/360152

1115775	MacOS agents cannot be updated to agent version 7.6 using the Global Agent update function under **System > Settings > Persistent Agent > Agent Update**.
	Upgrade Options:
	• Update Persistent Agent and Host Properties right-click options under **Users & Hosts > Hosts.**
	• Download the agent via the Captive Portal.
	• Push new agent package to macOS machines using a software management program. Note the following:
	  • Using this method will overwrite the agent settings. Both the package and the agent settings need to be pushed.
	  • If this process is used, then it should be used for all future agent updates and installations.
	For details on the above options, refer to sections Deployment Methods and Stage Agent for Deployment in the Persistent Agent Deployment and Configuration Guide.
	Update the agent manually on macOS machine. For instructions see Installation for macOS in the Administration Guide.

977586	Unable to download Mobile Agent from Google Playstore. Workaround: Download directly from the FortiNAC captive portal. For details, see Mobile Agent in the Administration Guide.
1101926	The resulting number of host records managed by Google GSuite MDM in the FortiNAC database is much smaller than the expected count. This is can occur if devices managed by GSuite are using shared docking stations or ethernet dongles. For details see article 370969.

Ticket #	Description
	https://community.fortinet.com/t5/FortiNAC-F/Technical-Tip-Duplicate-Ethernet-MAC-Addresses-result-in-small/ta-p/370969
1107531	High Availability configurations: RADIUS health check fails when the Require Message-Authenticator attribute is set to 'enable' under Network > RADIUS > Configuration. This causes the primary server to fail over to the secondary. For details and workaround see article https://community.fortinet.com/t5/FortiNAC-F/Troubleshooting-Tip-Require-Message-Authentication-set-to-Enable/ta-p/364116
1106999	Default AWS FortiNAC deployment script deploys with a data drive (disk) size of 10G. This must be increased to 100G prior to deployment. For details and workaround see article https://community.fortinet.com/t5/FortiNAC-F/Technical-Tip-How-to-prepare-the-FortiNAC-image-for-AWS/ta-p/376236
1057303	FortiNAC not generating events for "Invalid Physical Address" for VPN hosts using PA/DA Agents.
826653	FortiNAC supplied Dynamic Addresses on the FortiGate can become orphaned in FortiNAC High Availability environments. This can cause unintended network access.
1092462	Selecting "Resume Control" button multiple times in shot succession can potentially cause database corruption and prevent the restore to Primary from working properly.
1074050	Max allowed hosts per user is ignored when using 802.1x auto-registration.
1098205	FortiNAC sends logout/login messages in the same payload and it causes removing the user in the PALO ALTO user table.
1070325	Making changes in the older Model Configuration views (right-click model > Model Configuration) can override custom SSH port settings in the Credentials tab. Workaround: Make all changes using the newer Model Configuration and Credentials tabs at the top of the Inventory view.
1058705	No Support for Mixed FortiNAC-F (FortiNAC-OS) Appliance Types in High Availability Pair. See Requirements in High Availability guide for details.
954220	Unable to restore system backup files on FortiNAC-OS appliances.
875605	User search does not always not return user records as expected. Workaround: Use Legacy View.
827499	Show system interface does not accurately display port1/port2 IP sub Interfaces on FortiNAC-OS appliances. Workaround: Navigate to System > Config Wizard > Summary or run the following commands in the CLI: execute enter-shell ip addr
827283	The Roaming Guest Logical Network is missing from the Model Configuration of FortiGate and possibly from other vendors.

Ticket #	Description
1092085	root_SSL_VPN port gets switched to become a threshold uplink on modeled FortiGate. Workaround: Set root_SSL_VPN port to 'Never Uplink' in port properties.
1069869	Inventory Adapters section displays Caution sign when Persistent Agent is successfully communicating.

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).
	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 7.2.8

Ticket #	Description
1084926	D-LINK DGS-1210-28 3.01.003 D-LINK DGS-1210-20/C1 4.00.041 D-LINK WS6-DGS-1210-20/F1 6.10.007 D-LINK DGS-1210-28XS/ME/B2 Extreme Networks Switch Engine (5420F-48T-4XE-SwitchEngine) version 31.7.3.37 31.7.3.37 Extreme Networks, Inc. B5K125-48 Rev 06.81.08.0005 Extreme Networks Switch Engine (5320-24T-8XE-SwitchEngine) version 32.7.1.9 32.7.1.9 Huawei AR161F Huawei Versatile Routing Platform Software VRP HUAWEI CloudEngine S5735-L-V2 HUAWEI CloudEngine S5335-L-V2 Juniper Switch Cisco C9300 - 48 5Gbps UPOE ports (100M/1G/2.5G/5Gbps) Cisco Catalyst 1300 Series Managed Switch, 48-port GE, PoE, 4x1G SFP (C1300-48P-4G) Cisco Catalyst 1300 Series Managed Switch, 48-port GE, PoE, 4x10G SFP+ (C1300-48P-4X) Ruijie Gigabit Wireless Switch(WS6008)
1084091	Allied Telesis AT-GS950 V2 Series: atGS95010PSV2 atGS95018PSV2 atGS95028PSV2 atGS95052PSV2 Allied Telesis AT-X530L Series: atx530L28GTX atx530L28GPX atx530L52GTX atx530L52GPX atx530L10GHXm atx530L18GHXm
1078615	ArubaOS (MODEL: 503), Version 10.6.0.1-10.6.0.1 SSR Aruba S0E91A 6300M 48SR10 CL8 PoE 4p100G Sw FL.10.14.1000 Cisco Catalyst 1300 Series Managed Switch, 8-port GE, Ext PS, 2x1G Combo (C1300-8T-E-2G) Cisco IOS Software, CMICR Software (CMICR-UNIVERSALK9-M), Version 15.2(8)E3

Ticket #	Description
	Cisco IOS Software, IE2000 Software (IE2000-UNIVERSALK9-M), Version 15.2(7)E2 D-Link DES-3200-26 Fast Ethernet Switch D-LINK DGS-1210-28P/ME 6.00.025 D-LINK WS6-DGS-1210-08P/G1 7.30.004
1074187	Extreme Networks 5320-24T-8XE-FabricEngine (8.9.0.0) Extreme Networks Switch Engine (Stack) version 32.7.1.9 32.7.1.9 HPE Comware Platform Software, Software Version 7.1.070, Release 7639P02 HP 7503 JetStream 24-Port Gigabit L2 Managed Switch with 4 SFP Slots Meraki MS130-8X Cloud Managed PoE Switch Netgear 24-Port Gigabit Smart Switch with PoE and 4 SFP uplinks Netgear GS724TPP: 24-Port Gigabit Hi-Power PoE+ Ethernet Smart Managed Pro Switch with 2 SFP Ports and Cloud Management Omada 48-Port Gigabit L2 Managed Switch with 4 SFP Slots Ruckus Wireless R710 Arista Networks EOS version 4.29.2F running on an Arista Networks CCS-720DF-48Y-2 Cambium XE5-8 Five Radio Tri Band Wi-Fi 6E 8x8 High-Density Indoor Access Point with SDR Cisco CBS350-16T-2G 16-Port Gigabit Managed Switch Cisco CBS350-24FP-4X 24-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks Cisco CBS350-24FP-4X 24-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks Cisco CBS350-48FP-4G 48-Port Gigabit PoE Managed Switch Cisco IOS Software [Cupertino], C9800-AP Software (C9800-AP-K9_ IOSXE-UNIVERSALK9-M), Version 17.9.4 Cisco IOS Software [Dublin], C9800-AP Software (C9800-AP-K9_IOSXE-UNIVERSALK9-M), Version 17.12.3 Cisco SG250-18 18-Port Gigabit Smart Switch Dell EMC Networking N1148P-ON, 6.6.3.0 D-LINK DGS-1100-10MP Gigabit Ethernet Switch D-LINK DGS-1100-10MP Gigabit Ethernet Switch D-LINK DGS-1100-10MP Gigabit Ethernet Switch D-LINK DGS-1210-28/ME 6.11.R010B D-LINK DGS-1210-52/C1 4.10.004 D-LINK DGS-1500-28 1.00.013 D-LINK DGS-1510-28XMP Gigabit Ethernet SmartPro Switch D-LINK DGS-3100-24 Gigabit stackable L2 Managed Switch D-LINK WS6-DGS-1210-28MP/F1 6.30.016

Ticket #	Description
	D-LINK WS6-DGS-1210-52MP/F1 6.31.002
1065647	Aruba Wired Switch Aruba Wired Switch R8Q67A Juniper Switch Cisco NX-OS(tm) Nexus9300 C93180YC-FX3H, Software (NXOS 64-bit), Version 10.3(4a) Cisco NX-OS(tm) m9100, Software (m9100-s6ek9-mz), Version 8.2(1) Cisco 24-Port Gigabit Smart Switch OAW-AP1322 4.0.7 Meraki MS130-8P Cloud Managed PoE Switch Cisco IOS Software [IOSXE], IE31xx Switch Software (IE31xx-UNIVERSALK9-M), Version 17.13.1 Catalyst 1300 Series Managed Switch, 4-port 2.5GE, 4-port GE, PoE, 2x10G SFP+ (C1300-8MGP-2X)
1060520	Cisco SG250-50 50-Port Gigabit Smart Switch Cambium XV2-22H Two Radio Dual Band Wi-Fi 6 2x2 Wall Plate Indoor Access Point HUAWEI CE6810-32T16S4Q-LI HUAWEI S5700-52C-PWR-SI HUAWEI S2720-52TP-PWR-EI HUAWEI CloudEngine S6750-H HUAWEI CloudEngine S5735-L-V2 Cisco IOS Software, C800M Software (C800M-UNIVERSALK9-M), Version 15.9(3)M8 Allied Telesis router/switch, AW+ v5.4.6-0.1 Ruckus Wireless, Inc. ICX8200-24F, IronWare Version 10.0.10cT253 Meraki MS130-48P Cloud Managed PoE Switch
1058352	SNR SNR-S2985G-48T - Firmware Version 7.0.3.5(R0241.0472)
1058347	Zyxel XGS3700-24 - Firmware V4.30(AAGC.1)
1054376	HP Comware Platform Software, Software Version 5.20.99, Release 2108P07 HP A3600-48 v2 EI Switch CBS350-16P-E-2G 16-Port Gigabit PoE Managed Switch D-LINK DES-3552P Fast Ethernet Switch D-LINK DGS-F1210-26PS-E HW A1 Firmware V5.2.11.1 Cambium XV2-2 Two Radio Dual Band Wi-Fi 6 2x2 Indoor Access Point Aruba JL727B 6200F 48G CL4 4SFP+370W D-LINK WS6-DGS-1210-52/F1 6.20.007 Palo Alto Networks PA-1400

Ticket #	Description
	Cisco NX-OS(tm) Nexus9000 C9316D-GX, Software (NXOS 64-bit), Version 10.3(5) HPE Comware Platform Software, Software Version 5.20.99, Release 2112P05 HPE 3600-48-PoE+ v2 EI Switch
1050487	Cisco IE1000 Industrial Ethernet Switch, Version: 1.9.3
1026068	Allied Telesis Switches AT-x530l, AT-GS950
1018900	BoostLink SW, model - 701125

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	User Credentials required.
Password	Contact Support and reference KB article 291654.
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.**

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.