FortiNAC - Release Notes

Version F 7.6.6

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

Marth 5, 2026
FortiNAC F 7.6.6 Release Notes
49-922-769106-20211216

TABLE OF CONTENTS

Change log **4**
Overview of Version F 7.6.6 ..... **5**
Notes 5
Version Information 5
What's New in FortiNAC F 7.6.6 ..... **7**
Upgrade Requirements **8**
Upgrade path 8
Upgrade Considerations **10**
Hardware Support **12**
Pre-upgrade Procedure **13**
Compatibility **15**
Agents 15
Web Browsers for the Administration UI 15
Operating Systems Supported Without an Agent 15
Resolved Issues Version F 7.6.6 ..... **16**
Common Vulnerabilities and Exposures **17**
Known Issues Version F 7.6.6 ..... **18**
Device Support Considerations **20**
Device Support **21**
F 7.6.6 21
F 7.6.5 21
F 7.6.4 21
F 7.6.3 21
F 7.6.2 27
F 7.6.1 28
F 7.6.0 28
System Update Settings **30**
Numbering Conventions **31**

Change log

Date	Change description
November 13, 2025	Initial release.

Overview of Version F 7.6.6

- Build number: 0900

Notes

- Review the following sections prior to upgrading:
  What's New
  Upgrade Requirements
  Upgrade Considerations
  Pre-Upgrade Procedure
  Compatibility
  Known Issues
  Device Support Considerations
- To review software version information via CLI, type
  `get system status`
- For upgrade procedure, see OS and Software Upgrade posted in the Fortinet Document Library. Note the upgrade procedure has changed as of vF 7.6.3. This document now has two sections:
  Upgrade from a pre-F 7.6.3 version
  Upgrade from version F 7.6.3 or greater

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 7.6.6

Agent Version:

- MacOS/Linux — 10.7.2.13
- Windows — 9.4.4.105

Agents ship independent of product. For the latest Agent release notes, please see the Agent release notes.

- MacOS/Linux — 10.7.2.13
- Windows — 9.4.4.105

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.

What's New in FortiNAC F 7.6.6

No new features have been added in this release.

Upgrade Requirements

Ticket #	Description
1038485 1132649	High Availability / N + 1 Failover / FortiNAC Manager Environments. The following is required as of 7.6.0: Port 9443 must be open between FortiNAC appliances in order for inter-server communication to properly work. For a full list of open ports, see Open Ports section of the Administration Guide. Refer to the following sections: FortiNAC Access Configuration FortiNAC CA Firewall Policy Requirements FortiNAC Manager Firewall Policy Requirements
931408	Under **Portal > Portal SSL** the "Disabled" option is no longer available as of FortiNAC v9.4.5, vF7.2.5 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.
892856	High Availibility and FortiNAC Manager Environments. The following are required as of 7.2.2: 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.
875135	Environments using RADIUS Proxy: FortiNAC version F 7.4 updated the processing method FortiNAC uses to proxy RADIUS requests. This new enhanced method is referred to as the "Proxy RADIUS Service" and requires a different configuration. Existing RADIUS Proxy configurations in pre-7.4 FortiNAC releases will continue to work post upgrade and can be found under the "Legacy Proxy" view post upgrade. Review the Legacy Proxy section of the Administration Guide prior to upgrade for additional details.

Upgrade path

Important notice

FortiNAC F 7.6 only supports FortiNAC-OS. For CentOS migration to FortiNAC-OS, see CentOS to FortiNAC-OS migration documentation.

Current Version	Target Version	Upgrade Path Requirement	Ticket #
7.2 7.4	7.6	None	N/A
7.2	7.4	None	N/A

Upgrade Considerations

Ticket #	Description
	FortiNAC appliances running vF 7.6.3 on Google Cloud Platform (GCP) and Oracle Public Cloud (OPC) platforms: vF 7.6.4 will not display on the Latest tab under System > Settings > Updates > System at this time. **Workaround**: Look for it under All Upgrades tab. If not listed, upgrade using the File Upload tab. 1. In the Fortinet Customer Portal, navigate to https://support.fortinet.com/support/#/downloads/firmware 2. Select **FortiNAC-F** from Select Product drop-down menu. 3. Select Download tab. 4. Navigate to v7.00 > 7.6 > 7.6.4. 5. Download the applicable .out image by selecting the "HTTPS" link for the file: OPC: FNAC_OPC-v7-build0782-FORTINET.out GCP: FNAC_GCP-v7-build0782-FORTINET.out 6. Once downloaded, navigate to **System > Settings > Updates > System**. 7. Choose **File Upload** tab. 8. Click **+Browse** to upload the FortiNAC-OS firmware file. 9. Click **Upgrade** to continue with the installation.
1069751	FortiNAC Manager High Availability (HA) Pairs: The following changes will occur when upgrading from a pre-F 7.6 version to F 7.6.0 or greater: • HA configurations are replaced with the new Cluster Management feature: both Managers become active and manage the FortiNAC CAs. • VIP configurations are no longer supported and are removed. Note the VIP may still be reachable for up to 10 minutes post upgrade. • Above changes affect the FortiNAC Manager only...CAs are not affected. See What's New in 7.6.0.
1226034	High Availability: Upgrading from either F 7.6.3 or F 7.6.4 in a High Availability configuration removes the Secondary Server certificates. The certificates are no longer listed under **System > Certificate Management** for the Secondary. The behavior occurs if all following conditions apply: • FortiNAC is running version F 7.6.3 or F 7.6.4 • Separate certificates are used for the primary and secondary servers • Certificates are installed using a custom alias (Example: New EAP target)

Ticket #	Description
	For workaround see article Troubleshooting Tip: Secondary Certificates lost after upgrade.

Hardware Support

FortiNAC-OS is supported on legacy hardware.

This section lists the hardware models supported by FortiNAC F 7.6.

- 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 Procedure

Upgrading from FortiNAC version F 7.2.0 or F 7.2.1:

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.

New naming convention for agent package .jar file

Agent F 7.6.0 introduced a new naming convention for the agent package .jar file (FNACAgent-v7.6.x.xxxx.jar). The agent package filenames displayed will depend upon the FortiNAC version.

FortiNAC F 7.6.0, F 7.4.0, F 7.2.8 and lower: Only the older filename (agent*) is displayed.

FortiNAC F 7.6.1, F 7.4.1, F 7.2.9 and greater: Both filenames are displayed.

The FortiNAC versions that display both filename conventions for the same agent package can work with either one. For additional details, see Agent Release Notes.

https://docs.fortinet.com/document/fortinac-f/7.6.1/agent-release-notes/735428/download-agent-software

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	

Resolved Issues Version F 7.6.6

Ticket #	Description
1244725	Any duplicate MAC addresses in the database for host & adapter are now corrected when FortiNAC restarts.
1233513	FortiGate FortiOS 7.4.8 + unable to parse Dynamic Tag from FortiNAC.
1253864	Unable to process NetFlow sessions received from FortiGate.
1260261	Custom filter using the Device Type condition does not return any hosts.
1239749	FortiNAC Captive Portal Azure Entra-ID OAuth is not persistent.
1241303	Captive Portal does not redirect properly after changing portal 'Styles' when configured for User SAML SSO.
1236395	LDAP search not checking all directories if multiple Active Directories are added to FortiNAC.
1249719	FortiNAC stops responding to DHCP after the active server changes in High Availability pair. Workaround: DHCP service must be restarted.
1265191	Unable to discover FortiAPs managed by FortiGate when using duplicate IP addresses.
1249471, 1247369, 1250008	DataSyncer issue that caused FortiNAC logical business functionality to not work properly.

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.
- Applies to the FortiNAC-F product only (appliances running on FortiNAC-OS). Does not apply to FortiNAC appliances running on CentOS.

Bug ID	CVE References
1250490	OpenSSL - CVE-2025-15467

Known Issues Version F 7.6.6

Ticket #	Description
1250008	Unable to run backups in FortiNAC vF 7.6.5. For details and workaround see article https://community.fortinet.com/t5/FortiNAC-F/Technical-Tip-Unable-to-run-backups-in-FortiNAC-vF-7-6-5/ta-p/429650.
1251817	Updating ports/switching VLANs on a FortiSwitch in FortiLink mode fail if FortiNAC is sending access tokens in the URL to the managing FortiGate. Additionally, the API token is removed from the FortiGate's Model Configuration. Affects FortiGates running FortiOS version 7.4.5+ or 7.6.1+. For details and workaround see article https://community.fortinet.com/t5/FortiNAC-F/Technical-Tip-Configure-FortiGate-v7-4-5-v7-6-1-to-allow-access/ta-p/429325
1238368	If a logged on user is added to a host record via non-RADIUS method, the logged on user is removed if a RADIUS request is received which doesn't include the user for that host.
1222719	FortiNAC not sending RADIUS CoA to Huawei wireless controller - failed adding 44 to attribute list.
1207426	Unable to discover sites managed by Huawei Cloud.
1165259	Agent Communication delay for devices connecting to new ASA.
1185734	FortiNAC 7.6 does not display all group members in GUI.
1211434	Users and Hosts > Applications shows a very large number of entries.
1220655	Scan-on-Connect initial scan not running subsequent scans defined in Override Scan Result Actions.
1236395	FortiNAC only checks first LDAP server and rejects RADIUS request, although LDAP groups are selected from second LDAP server.
1236584	DHCP scopes can no longer be edited after entering an invalid scope.
1075030	CLI DeviceImport is failed when csv-file include "#".
1174765	Login process does not complete for Android/iOS devices when using Azure Portal.
1208434	Cannot register in Captive Portal using User SAML SSO Auth due to redirects.
1210843	"Additional Access Values" values missing.
1211401	FortiNAC with "Enable Quarantine VLAN Switching" unchecked keeps moving endpoint to Quarantine VLAN for Wireless users.
1212020	FortiNAC does not maintain the "Discovery Settings" credentials and IP.

Ticket #	Description
1220088	Bulk edit no longer available in Network > Inventory view.
1220713	FortiNAC does not list all hosts managed by Google GSuite MDM.
1225545	VLANs are not synchronized for MR46 Meraki.
1226482	Device profiling rule matches but does not register host.
1171477	Self Registration template for sponsor approval results in Phishing email
1205127	Installing a new license key with a different serial number than the existing key on FortiNAC Manager VM's is currently not supported. Most commonly seen in environments where a license has expired and a new license must be registered and installed. This causes unexpected behavior in FortiNAC manager. For details and workaround see article https://community.fortinet.com/t5/FortiNAC-F/Troubleshooting-Tip-New-license-key-with-different-serial-number/ta-p/422930
1190679	Deny/Enforce RADIUS Access Enforcement options display in the Model Configuration for devices that are not configured for RADIUS.
1164322	Captive Portal taking longer than expected to load pages and complete the process.
1171477	Self Registration template for sponsor approval results in Phishing email.

Device Support Considerations

Ticket #	Description
1238211	FortiNAC currently does not support MAC-AGED notification trap from Aruba JL255A 2930F-24G-PoE+-4SFP+
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).
860546	L3 Polling currently not supported on Extreme Wireless Controllers
	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

F 7.6.6

This release does not introduce additional device support.

F 7.6.5

Ticket #	Description
1151372	Cisco 9800 AP WLC
1174678	Allied Telesis Switches (AT-IE340-20GP-980 / AT-IE220-10GHX-980 / AT-IE220-6GHX-980)
1168898	Dahua S4228-24GT-360 , IS4420-16GT-240 Switches
1092940	TP-Link Switch TL-SG3428
1077148	Dell Switches Running Dell Sonic OS

F 7.6.4

There is no new device support in FortiNAC F 7.6.4

F 7.6.3

Ticket #	Description
1157986	Cisco IOS Software, IE2000 Software (IE2000-UNIVERSALK9-M), Version 15.2(7)E2, RELEASE SOFTWARE ExtremeXOS (X435-24T-4S) version 30.6.1.11 30.6.1.11 ExtremeXOS (X435-24P-4S) version 30.7.1.1 30.7.1.1-patch1-86 ExtremeXOS (X460G2-24t-G4) version 16.1.2.14 16.1.2.14 Huawei YunShan OS Version 1.22.1.1 (S5700 V600R022C10SPC500) HUAWEI CloudEngine S5735-L-V2 Huawei YunShan OS Version 1.23.1.1 (S5700 V600R023C10SPC500) HUAWEI CloudEngine S5735-S-V2

Ticket #	Description
	Huawei YunShan OS Version 1.24.0.1 (S8700 V600R024C00SPC500) HUAWEI CloudEngine S8700-4 Huawei YunShan OS Version 1.23.1.1 (S5700 V600R023C10SPC500) HUAWEI CloudEngine S5735-S-V2 Juniper Networks, Inc. ex4000-12mp Ethernet Switch, kernel JUNOS 24.4R1.12 Meraki MS150-24P-4X Cloud Managed PoE Switch HP 1810-8 Aruba Instant On 1830 8G Switch JL810A, InstantOn_1830_2.6.0.0 (73)
1152321	Model FortiPAM Correctly in NW Inventory
1149495	Arista Networks EOS version 4.32.3M Arista Networks EOS version 4.33.1.2F Meraki MS130-48X Cloud Managed PoE Switch Catalyst 1300 Series Managed Switch, 16-port GE, PoE, 2x1G SFP (C1300-16P-2G) Allied Telesis router/switch, Software (AlliedWare Plus) Version 5.5.2-2.7 Ruijie Gigabit Ethernet Switch with PoE (S2915-10GT2MS-P-L) CBS250-8P-E-2G 8-Port Gigabit PoE Smart Switch AlliedWare Plus (TM) 2.2.4.0 SNR-S2982G-24TE Device, SoftWare Version V702R101C013 Cisco IOS Software, C860 Software (C860VAE2-ADVSECK9-M), Version 15.6(3)M3a Catalyst 1200 Series Smart Switch, 48-port GE, PoE, 4x10G SFP+ (C1200-48P-4X) Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_ IOSXE), Version 17.10.1prd7 Huawei AR617VW Huawei Versatile Routing Platform Software VRP (R) software,Version 5.170 (AR610 V300R022C00SPC100) Huawei AR6140-9G-2AC Huawei Versatile Routing Platform Software VRP (R) software,Version 5.170 (AR6140 V300R019C10SPC600) Arista Networks EOS version 4.32.5M running on an Arista Networks CCS-720XP-96ZC2-M-S
1147421	Cisco Switches C9200L-48P-4X & C9200L-24P-4X.
1137795	Aruba Instant On 1960 48G 40p Class4 8p Class6 PoE 2XGT 2SFP+ 600W Switch JL809A Cisco Wireless CW9176I Cloud Managed AP Palo Alto Networks PA-3400 series firewall Extreme Networks ExtremeCloud IQ Controller - VE6120H Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_LITE_ IOSXE)

Ticket #	Description
	HPE ANW JL724B 6200F 24G 4SFP+ HPE 5710 48SFP+ 6QS+/2QS28 Huawei S5735-L24P4X-A Alcatel-Lucent Enterprise OS6860E-48
1134269	Yamaha Switch SWX2310
1132005	ApresiaNP2000-48T4X Gigabit Ethernet Switch Ver.1.07.01 APLFM104GTPOE Fast Ethernet Switch ApresiaNP2100-24T4X Gigabit Ethernet Switch Ver.1.10.05 ApresiaNP2500-16MT4X-PoE Gigabit Ethernet Switch Ver.1.08.04 Cambium XV2-21X Two Radio Dual Band Wi-Fi 6 2x2 Indoor Access Point Meraki MS130-8P-I Cloud Mgd 8GE 120W PoE Switch Meraki CW9166D1 Cloud Managed AP ApresiaNP4000-20Xt4X TenGigabit Ethernet Switch Ver.1.03.01 Linux fwinterno01 3.10.0-957.21.3cpx86_64 1 SMP SG550X-24MPP 24-Port Gigabit PoE Stackable Managed Switch C9300 - 40-port 5G/mGig, 8-port 10G, Modular Uplinks, UPOE+ Meraki MS130-48 Cloud Managed Switch
1129868	Cisco Meraki C9300-24
1126332	FortiNAC - EMS Cloud integration
1124109	ALAXALA AX2340S AX-2340-24T4X-B [AX2340S-24T4X] Switching software Ver. 2.6 DGS-1210-52 3.10.013 Juniper Networks, Inc. ex4100-48t Ethernet Switch, kernel JUNOS 22.4R3.25, Cisco IOS Software, C1530 Software (ap1g3-K9W7-M), Version 15.3 (3)JF4 Ruckus Wireless Inc (C) 2006 Catalyst 1300 Series Managed Switch, 16-port GE, PoE, 4x10G SFP+ (C1300-16P-4X) C9300 - 48 Cisco UPOE 36x 100M/1G/2.5G + 12x Multigigabit (100M/1G/2.5G/5G/10Gbps), Modular Uplinks C9300 - 12 1G/10G/25G SFP28, Modular Uplinks APLFM108GTSS Fast Ethernet Switch APLFM116GTSS Fast Ethernet Switch ApresiaNP2500-8MT4X-PoE Gigabit Ethernet Switch Ver.1.10.03 FG121G FG91G C9300 - 48 POE+, Modular Uplinks JetStream 10-Port Gigabit Smart Switch with 8-Port PoE+

Ticket #	Description
	JetStream 24-Port Gigabit L2 Managed Switch with 4 SFP Slots DGS-1210-52/ME 4.00.R033
1116472	Yamaha Router NVR510
1111434	ArubaOS (MODEL: 575), Version 10.7.0.0-10.7.0.0 ArubaOS (MODEL: 655), Version 10.7.0.0-10.7.0.0 SSR Huawei AP5030DN-S ALAXALA AX2340S AX-2340-24T4X-B [AX2340S-24T4X] Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.5(2)T Cisco C2960L Software (C2960L-UNIVERSALK9-M) Cisco C2955-I6Q4L2-M Alcatel-Lucent Enterprise OS6360-P48 FS.COM INC switch RUGGEDCOM INC Cambium XE3-4 Three Radio Tri Band Wi-Fi 6E 4x4 Indoor Access Point with SDR Arista Networks CCS-720DP-48S-2 Ruckus Wireless, Inc. Stacking System ICX7550-48F ALLIED TELESIS INC. AT-GS950/16PS Gigabit Ethernet WebSmart Switch
1108503	Hybrid port support in Ruijie switches
1106401	Meraki MS390-48U L3 Stck Cld-Mngd 48-port GbE UPoE switch HP J9856A 2530-24G-2SFP+ Switch, revision YA.16.11.0013 Meraki CW9163E Cloud Managed AP C9300 - 48 Cisco UPOE, Modular Uplinks Fortinet FS-AX2630S FS-AX2630S-24T4XW [FS-AX2630S-24T4XW] Switching software Ver. 2.5 [OS-L2N] S5700-52X-PWR-LI-AC Huawei Versatile Routing Platform S6720-54C-EI-48S-AC Huawei Versatile Routing Platform S5720-52X-PWR-SI-ACF Huawei Versatile Routing Platform Juniper Networks, Inc. ex4400-24mp Ethernet Switch S5720-36C-EI-AC Huawei Versatile Routing Platform S5720-36C-EI-28S-AC Huawei Versatile Routing Platform S5732-H48S6Q Huawei Versatile Routing Platform Catalyst 1300 Series Managed Switch, 48-port GE, Full PoE, 4x10G SFP+ (C1300-48FP-4X) Catalyst 1300 Series Managed Switch, 8-port GE, Full PoE, 2x1G Combo (C1300-8FP-2G)
1102795	AX3660S

Ticket #	Description
1099808	Netgear GS110TPv3 8-Port Gigabit Smart Managed Pro Switch with PoE+ and 2 SFP Ports Netgear GS724TPv2 ProSAFE 24-Port Gigabit Smart Managed Switch with PoE+ and 2 SFP Ports HPE Comware Platform Software, Software Version 7.1.070, Release 2719P01-US HPE FF 12902E Cisco CBS350-16T-E-2G 16-Port Gigabit Managed Switch Cisco Catalyst 1300 Series Managed Switch, 8-port GE, PoE, Ext PS, 2x1G Combo (C1300-8P-E-2G) Cisco 24-Port 10/100 PoE Stackable Managed Switch Cisco IOS XR Software (NCS-5500) Huawei S5735-L48T4X-A Huawei S5735-L8P4S-QA1 Alcatel-Lucent Enterprise OS6360-P48X Palo Alto Networks PA-3400 series firewall
1095424	Netgear 24-Port Gigabit Smart Switch with PoE and 4 SFP uplinks ArubaOS (MODEL: 735), Version 10.7.0.1-10.7.0.1 SSR Catalyst 1300 Series Managed Switch, 8-port 10GE, 8-port SFP+ (C1300-16XTS) H3C S5120V3-52S-PWR-LI Cisco IOS Software, CDB Software (CDB-UNIVERSALK9-M), Version 15.2(7)E3 D-Link DES-3052P Fast Ethernet Switch D-Link DGS-1210-28P
1092033	Cisco 9300L-48UXG-4X
1092032	Cisco 9300L-48PF-4X When Managed by Meraki Cloud
1089864	Fortinet Extreme Networks Switch Engine (5420F-48P-4XE-SwitchEngine) Ruijie AP680(CD) (802.11a/n/ac/ax and 802.11b/g/n/ax) Extreme Networks Switch Engine (5420M-48W-4YE-SwitchEngine) Aruba Instant On 1930 24G Class4 PoE 4SFP/SFP+ 195W Switch JL683B Juniper Networks, Inc. qfx10002-36q Ethernet Switch, kernel JUNOS 22.2R3.15 Juniper Networks, Inc. srx320 internet router, kernel JUNOS 20.2R3-S4.7
1087220	OmniSwitch 2260 and 2360
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

Ticket #	Description
	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
1081031	Expanded Generic SNMP Integration VLAN Switching Capabilities
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

Ticket #	Description
	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 D-LINK WS6-DGS-1210-52MP/F1 6.31.002
1069705	Allied Telesis Switch MAC-notification trap support
1067283	FutureMatrix S5735 Switch
1055634	Ubiquity Gen2 Switch Unifi USW 24 PoE
1038457	ExtremeXOS X440G2-12p-10G4

F 7.6.2

Ticket #	Description
1065647	Aruba Wired Switch Aruba Wired Switch R8Q67A Juniper Switch

Ticket #	Description
	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)
1058352	SNR SNR-S2985G-48T - Firmware Version 7.0.3.5(R0241.0472)
1058347	Zyxel XGS3700-24 - Firmware V4.30(AAGC.1)

F 7.6.1

Ticket #	Description
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 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

F 7.6.0

See also Device Support for Versions:

- F 7.2.7
- F 7.4.0

Ticket #	Description
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 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
1026068	Allied Telesis Switches AT-x530l, AT-GS950
1018900	BoostLink SW, model - 701125

System Update Settings

This page is only available in FortiNAC versions prior to F7.6.3 as the GUI has changed. For details regarding the new page, see System in the 7.6 Administration guide.

See also the OS and Software Upgrade guide.

Provides two sets of instructions based upon the currently running FortiNAC version:

Upgrade from a pre-F 7.6.3 version

Upgrade from version F 7.6.3 or greater

Applies to FortiNAC systems running vF 7.6.2 and below.

FortiNAC version vF 7.6.3 and above no longer use this view for downloading images. This page has been replaced with "System". For details about this page, see System in the Administration Guide.

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_6
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.**

Numbering Conventions

Fortinet is using the following version number format:

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

Example: F 7.6.6.0900

- 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.