FortiNAC - Release Notes

Version F 7.2.9

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

May 9, 2025
FortiNAC F 7.2.9 Release Notes
49-922-769106-20211216

TABLE OF CONTENTS

Change log

Date	Change description
May 9, 2025	Initial release.

Overview of Version F 7.2.9

- Build number: 0166

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 7.2.9

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	7.2.9	None	N/A
7.2.1			
7.2.2			
7.2.3			
7.2.4			
7.2.5			
7.2.6			
7.2.7			
7.2.8			

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 7.2.9 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.

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	

What's New in F 7.2.9

Update Host Role Based on MDM Device Ownership

Applies to Microsoft InTune, Air Watch, MaaS360, Mobile Iron, and Citrix MDM integrations.

Administrators are now able to build policies based on Device Ownership values stored in MDM records. FortiNAC reads the Device Ownership attribute associated with the MDM managed endpoint and updates its Host role to match. Feature is optional. For details, refer to the following documentation:

MDM Servers in the Administration Guide

MDM/OT Security Integration

Resolved Issues F 7.2.9

Ticket #	Description
1149169	Primary would fail over to Secondary when Admin UI (8443) port takes a long time to become available.
1146655	NCM/Manager will not load the server list, which persists after restarts.
1144996	unauthorized_scope_error in LinkedIn oAuth2 authentication' displayed in portal.
1144542	CLI Configuration Schedule Task does not log an Event Log.
1140386	hsRestartCMMaster command does not resume control of High Availability pair.
1139952	More efficient SSH communication between FortiNAC and Cisco ASA, requiring fewer connections.
1139824	Reduced the time it takes for FortiNAC Server to start.
1136380	Multiple 'Host destroyed' events, causing host to be isolated.
1136018	High Availability database replication not working due to inconsistent permissions for user 'bsiadmin'@'localhost'.
1133876	The secondary server does not display the correct concurrent license count in GUI (System > Settings > System Management > License Management). **Resolution**: When the secondary is in standby, License Name and Concurrent Licenses fields will now display INHERITED FROM PRIMARY. See High Availability guide for details.
1133813	Migrated legacy device types cause error when bulk importing hosts.
1132680	Unable to Increase Allowed Host Limit using Modify User Dialog on Manager.
1129743	RADIUS - Clean install - Attribute dictionary populates standard attributes with bogus vendor on a new installation.
1129706	Custom Script Success' event sent to FortiAnalyzer is truncated.
1128684	Guest-conference account shared credentials: Second guest gets an error: "Login Failed: Registered Client Not Found".
1126001	Control server fails over after upgrade to 9.4.8 due to failing health check.
1124477	Opening "Model Configurations" by right-clicking the appliance in FortiNAC's Inventory shows HTTPS Status 500 - Internal Server.
1122400	Newly added FortiSwitch in FortiLink mode is missing Port Attributes.
1120645	Portal is redirecting to /authentication/Success.jsp even when there is a LogOff/deauthentication process.

Ticket #	Description
1118281	Manually adding MAC addresses with '-' as delimiter prevents the DHCP service in FortiNAC from starting.
1116162	Test SSH connection for remote backup displays an incorrect error message.
1114927	Copying styles only from Portal A to Portal B copies all content, settings and styles.
1114796	The following events are missing in the Trigger event drop-down menu under Logs > Events & Alarms > Mappings: Unauthorized Connection from FortiNAC Appliance Unauthorized Connection from legacy FortiNAC Appliance
1113461	MS Intune MDM integration not pulling in Ownership information.
1110661	Host Groups User information is lost when LDAP synchronization is run.
1110655	Unable to change the MDM polling timer once configured.
1110289	Winbind Error when adding a second domain using special characters.
1110127	"Portal Configuration" tab does not load due to FortiNAC unable to resolve www.fortinet.com.
1109849	Intermittent L2/L3 polling failures with Mist AP.
1109710	Hardware appliances in High Availability: Secondary server can not get subscription license entitlements from primary server.
1109467	Hosts > Policy Details > Network Access shows policy matched whereas RADIUS log shows no network access policy match found.
1109325	FortiNAC unable to remove LDAP Admin user after Directory sync, while user is already removed in AD group.
1109181	802.1x:EAP-TLS: Host placed initially in Registration VLAN then placed in production VLAN with 802.1x Auto Registration.
1108957	Unable to select radius attribute "User-Name" in Network>Radius>Attribute Groups.
1108503	Support for hybrid ports in Ruijie switches.
1108177	Admin UI service health check failure triggers failover in High Availability pair.
1107826	Agent Server service health check failure triggers failover in High Availability pair.
1107750	Error returned when running FortiNAC-OS CLI command 'get hardware nic' in AWS deployment.
1107531	RADIUS service health check failure triggers failover in High Availability pair.

Ticket #	Description
1106999	Default AWS FortiNAC deployment script deploys 10G of memory which cannot be changed.
1105674	Validate Credentials and Device Mapping not working for a Cisco Switch Catalyst 1200 Series.
1104997	Global nested groups are not displayed after FortiNAC CA restarts.
1104149	SSH connection failure when modeling VIP using the MultiKnownHostEntries feature.
1104143	Device Profiling Rule not matching using Windows Profile method.
1099315	Connected Container is showing incorrect information in the Port Adapter detail.
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
1098758	Unable to read or change VLANs on D-LINK DGS-F1210-26PS-E.
1098689	L2 polling is failing for Huawei WLC.
1098205	FortiNAC sends logout/login messages in the same payload and it causes removing the user in the PALO ALTO user table.
1093529	MS-intune integration Test Connection and Polling failed.
1092462	Selecting "Resume Control" button multiple times in shot succession can potentially cause database corruption and prevent the restore to Primary from working properly.
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.
1091748	Aruba WLC hosts do not change network access after a host state change.RADIUS CoA disconnect not working as expected.
1087717	Improvements to the FortiNAC System Backup function: - Write full CLI configuration (show full configuration) to file <hostname>.<yyyymmdd>.show-full-configuration.gz - Restore full CLI configuration using 'execute restore config'
1087398	FortiNAC unable to make changes on Aruba 3200 F Cloud controlled aruba switches.
1084559	FortiNAC unable to login to CLI ofKyland 3024P Switch causing L2 Poll and VLAN change failures.

Ticket #	Description
1083981	New RADIUS health check causes repeating login reject in post-auth in RADIUS log every 30 seconds.
1081023	RADIUS authentication failing for TLS1.0/1.1 due to "no suitable signature algorithm".
1078055	FortiNAC not sending RADIUS CoA to Huawei switch.
1075669	FortiNAC not sending RADIUS CoA to Aruba Switch 6200 OS-CX.
1074050	Max allowed hosts per user is ignored when using 802.1x auto-registration.
1070462	Conference account with Max Attendees 1 allows 2 registrations.
1069664	L2 Polling fails with Ubiquiti AP.
1058705	No Support for Mixed FortiNAC-F (FortiNAC-OS) Appliance Types in High Availability Pair. See Requirements in High Availability guide for details. https://docs.fortinet.com/document/fortinac-f/7.2.0/high-availability-fortinacos/299094/overview
1057303	FortiNAC not generating events for "Invalid Physical Address" for VPN hosts using Persistent or Dissolvable Agents.
1030100	Wired connection action state values set to "Bypass" via API display as "Enforce" in GUI.

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
1155879	FortiNAC F x.x.x is not vulnerable to the following CVE reference because FortiNAC does not enable the DisableForwarding directive. • CVE-2025-32728
1092986	FortiNAC F 7.2.9 and greater is no longer vulnerable to the following CVE reference. • CVE-2023-27522 • CVE-2024-27316 • CVE-2024-38476 • CVE-2024-38477

Bug ID	CVE references
1060728	FortiNAC F 7.2.9 and greater is no longer vulnerable to the following CVE reference. • CVE-2024-4076 • CVE-2024-1975 • CVE-2024-1737 • CVE-2024-0760
1051904	FortiNAC F 7.2.9 and greater is no longer vulnerable to the following CVE reference. • CVE-2024-6387

Known Issues F 7.2.9

Ticket #	Description
1136654	'Host CLI Task Success' event not generated when the Undo in CLI Configuration is executed during manual registration.
1165259	Agent Communication delay for devices connecting to new ASA.
1217904	FortiNAC CA loses license entitlements after communication timeout with FortiNAC Manager.
1174765	Login process does not complete for Android/iOS devices when using Azure Portal.
1211401	FortiNAC with "Enable Quarantine VLAN Switching" unchecked keeps moving endpoint to Quarantine VLAN for Wireless users.
1225545	VLANs are not synchronized for MR46 Meraki.
1171477	Self Registration template for sponsor approval results in Phishing email
1203457, 1219523	Session based API login is failing in FortiGate integrations running FortiOS 7.6.4. This prevents FortiNAC from managing the FortiGate properly. Symptoms include errors and display issues in Inventory for the FortiGate and FortiSwitch in FortiLink mode. **Workaround**: Use token based API access. See article for instructions https://community.fortinet.com/t5/FortiNAC/Technical-Tip-How-to-configure-amp-use-API-token-to-communicate/ta-p/297192
1168135	Unable to edit Kiosk pages on FortiNAC-OS appliances.
1188296	Running multiple simultaneous downloads while using Firefox can generate errors. Downloads may not complete. Example: Exporting hosts to CSV file while downloading logs.
1163996	Hardware migration does not complete on FortiNAC appliances with two ports. For details see article https://community.fortinet.com/t5/FortiNAC-F/Troubleshooting-Tip-Hardware-Migration-does-not-complete-on/ta-p/394903
924474	When creating Groups on FortiNAC, SSIDs are not shown under FortiLAN Cloud container. FortiAP is not under the FortiLAN network.
1007605	Performance issues with adding/updating the host
1147758	Unable to poll Microsoft Intune MDM when "Enable Compliance Retrieval Status" is enabled.
1148175	Uploading portal images beyond the max size of 1 MB displays "There was an error processing this request".

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

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. https://community.fortinet.com/t5/FortiNAC-F/Technical-Tip-Duplicate-Ethernet-MAC-Addresses-result-in-small/ta-p/370969
826653	FortiNAC supplied Dynamic Addresses on the FortiGate can become orphaned in FortiNAC High Availability environments. This can cause unintended network access.
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.
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:

Ticket #	Description
	execute enter-shell ip addr
827283	The Roaming Guest Logical Network is missing from the Model Configuration of FortiGate and possibly from other vendors.
1069869	Inventory Adapters section displays Caution sign when Persistent Agent is successfully communicating.

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).
	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 C5LI 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 7.2.9

Ticket #	Description
1038457	ExtremeXOS X440G2-12p-10G4
1092032 1092033	Cisco 9300 switches managed via the Meraki Cloud.
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) HPE ANW JL724B 6200F 24G 4SFP+ HPE 5710 48SFP+ 6QS+/2QS28 Huawei S5735-L24P4X-A Alcatel-Lucent Enterprise OS6860E-48
1129868	Cisco Meraki C9300-24
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
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

Ticket #	Description
	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
1100922	Fortigate 70F being mapped as Fortigate 70D
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
1089864	Fortinet

Ticket #	Description
	Extreme Networks Switch Engine (5420F-48P-4XE-SwitchEngine) 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
1067283	Huawei FutureMatrix Series Switches
1055634	Ubiquity Gen2 Switch
971269	Alcatel OAW-AP1221 Access Points

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.